

## MEMO

**TO:** Colorado Department of State [SOS.Rulemaking@sos.state.co.us](mailto:SOS.Rulemaking@sos.state.co.us)  
**FROM:** Colorado Voter Group  
**DATE:** May 13, 2015  
**SUBJECT:** Response to your request, "Help Shape Colorado's Election Rules, May 8, 2015"

**Documents copied here for your information:**

1. Verified Voting opposition to House Bill 1130 (p. 2–3)
2. Security Considerations for Remote Electronic UOCAVA Voting (NISTIR 7770; p. 4–74)
3. Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters (NISTIR 7711; p. 75–147)
4. Information System Security Best Practices for UOCAVA Supporting Systems (NISTIR 7682; p. 148–191)
5. A Threat Analysis on UOCAVA Voting Systems (NISTIR 7551; p. 192–269)
6. Risks of Internet Voting, by Barbara Simons (p. 270–271)
7. Hazards of Email Voting, by David Jefferson (p. 272–276)
8. Dynamic Authentication: Smarter Security to Protect User Authentication (IDC 1777; p. 277–282)

Colorado Voter Group thanks you for the invitation to help shape Colorado's election rules. Please include our response and the documents copied here into the list of publicly provided responses.

To achieve your stated objectives, you will need a much more robust rule than that referenced in your May 8<sup>th</sup> request. The development of such a robust rule would necessarily require an improved process designed to fully exploit the knowledge and experience of the public, and that would place CDOS administrators and staff in a position to defend the proposed rule.

One illustration of this need is proposed rule 16.2.1(c), concerning electronic transmission.

The Secretary of State is the executive office that is legally accountable for ensuring the purity of elections. The adoption of proposed rule 16.2.1(c) can, and most probably would, result in the contamination rather than the purification of future elections.

We ask that you promptly disclose and publicly defend your written rebuttals to each of the enclosed written arguments against Internet voting, and your evidence proving that adopting this rule would not contaminate future elections.

Without such evidence, peer reviewed and publicly defended, it would be irresponsible for the department to proceed with adoption of this rule.

We ask that you negotiate with the public to develop an improved rulemaking process that would achieve the above stated objectives.

We are available to participate in such a public debate.

*Al Kolwicz*

**Colorado Voter Group**

[REDACTED]  
[REDACTED]

[www.ColoradoVoterGroup.org](http://www.ColoradoVoterGroup.org)  
<http://coloradovoter.blogspot.com>



March 23, 2015

Senator Bill Cadman  
 Senator Mark Scheffel  
 Senator Morgan Carroll  
 Senator Rollie Heath

Honorable Senators: We write today to express our opposition to House Bill 1130, a bill that as amended would expand the practice in Colorado of return of voted ballots by electronic transmission over the Internet. Verified Voting is a national, non-partisan, nonprofit committed to safeguarding democracy in the digital age, with many Colorado supporters. We advocate for voting technology and policies that promote and improve transparency, accessibility, security and auditability in the election process.

There is a common misconception that returning voted ballots via email as PDF attachments and printing them for scanning at a central scanner is not Internet voting, and somehow does not introduce the security risks of “Internet voting.” This is misleading. Marked or “voted” ballots returned by electronic means (including but not limited to email in the form of PDF attachments) are vulnerable to tampering, manipulation, deletion, and eavesdropping as they travel the Internet, before they can be printed at the elections office. It is not merely the tabulation of votes that must be protected from the risks of the Internet, but the votes themselves even before they can arrive to be tabulated.

The National Institute of Standards and Technology (NIST) is the federal agency tasked with researching the security considerations of voting technology including for remote electronic UOCAVA voting. In examining the email return of voted ballots NIST found that **voted ballots returned by email are vulnerable to privacy violations and malicious tampering at countless points as they travel over unsecured networks and email servers.**<sup>i</sup> NIST also warned that voter’s computers may be infected with malicious code or “**malware**” that could modify ballots before they are emailed to the election official. Malware could also infect the election computer system and modify ballots before they are printed. In either case, even if the malware was discovered before Election Day, election officials have **no way to identify affected ballots.**<sup>ii</sup> This sort of attack, they warn, could be orchestrated by updating malware on already infected computers to recognize and attack ballots and therefore could have large-scale impact.<sup>iii</sup>

NIST also points out email ballot transmission is “significantly **easier to intercept and modify in transit** than other forms of communication.”<sup>iv</sup> This is borne out by other experts: Brian Hancock of the U.S. Election Assistance Commission states: “Email is about the least secure method of ballot delivery.”<sup>v</sup> Earlier this year researchers at Galois, a defense contractor and computer security firm, published a technical paper detailing an example of an attack on ballots returned by email.<sup>vi</sup>

The solution is as a Federal Voting Assistance Program (FVAP) report to Congress states: “Electronic delivery of a blank ballot, when **combined with the postal return of the voted ballot, remains the most responsible method** for moving forward until such time applicable Federal security guidelines are adopted by the [U.S. Election Assistance Commission].” FVAP is responsible for assisting military and overseas voters to ensure their ability to participate effectively in elections.

Colorado permits the insecure practice of electronic return of voted ballots by email return for UOCAVA voters—but in limited circumstances. CO Rev. Stat. 1-8.3-113 states this can happen, for voters who requested their ballots electronically:

*(1) (a) In circumstances where another more secure method, such as returning the ballot by mail, is not available or feasible, as specified in rules promulgated by the secretary of state; or (b) If the ballot is for a recall election conducted under article 12 of this code.*

Thus far, we have been unable to find any guidance or rule the Secretary of State may have promulgated to ensure that the more secure method of returning voted ballots is used (cf. Election Rules 8 CCR 1501-116). Given the forgoing guidance, postal mail return should trump email ballot return.

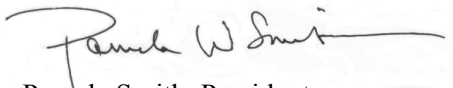
In agreement with the Military and Overseas Voter Empowerment (MOVE) Act and the Uniform Law Commission's Uniform Military and Overseas Voter Act (UMOVA), Colorado provides blank ballots electronically and 45 days before an election to military and overseas voters. Colorado also wisely allows military ballots to be counted as long as they are postmarked on Election Day and received up to eight days after the election. Military voters are entitled to expedited postal mail return of voted ballots at no cost, which are returned to election officials within 5.2 days on average. These are significant steps that ease and facilitate the voting process for military and overseas voter and we commend you for those provisions.

In addition, we strongly believe all ballots, including those of our men and women in uniform, deserve to be transmitted securely and privately. *We oppose the provision in HB 1130, which we understand was added in Committee after introduction, that therein expands online return of voted ballots. We have no position on the other provisions of the bill.*

We also urge the legislature, in light of daily revelations of the comprehensive lack of security of the Internet for any purpose as important as the transmittal of votes, to consider repealing the return of voted ballots by electronic means, before the inevitable corrupted election occurs. Until then, we will work with the Secretary of State to develop clear and specific rules governing the return of voted ballots in agreement with Colorado statute 1-8.3-113.

Thank you very much for your consideration and attention to this matter.

Very truly yours,



Pamela Smith, President  
VerifiedVoting.org

Cc: Senator Leroy Garcia  
Kjersten Forseth

---

<sup>i</sup> NIST IR 7551 "A Threat Analysis of UOCAVA Voting systems" <http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf>

<sup>ii</sup> Ibid.

<sup>iii</sup> NIST IR 7700 "Security Considerations for Remote Electronic UOCAVA Voting." "While each successful attack on the client can only impact one vote or voter (or potentially a small number of voters if a computer is shared), attackers have demonstrated an ability to infect a large number of clients, and thus client-side attacks have the ability to have a large-scale impact."

<sup>iv</sup> NIST IR 7551

<sup>v</sup> "Internet Voting – Not Ready for Prime Time?" National Conference of State Legislatures, *The Canvass*, Feb 2013 [http://www.ncsl.org/Documents/legismgt/elect/Canvass\\_Feb\\_2013\\_no\\_37.pdf](http://www.ncsl.org/Documents/legismgt/elect/Canvass_Feb_2013_no_37.pdf)

<sup>vi</sup> <https://galois.com/blog/2014/11/hacking-internet-voting-via-ballot-tampering/>

**NISTIR 7770**

# **Security Considerations for Remote Electronic UOCAVA Voting**

Nelson Hastings  
Rene Peralta  
Stefan Popoveniuc  
Andrew Regenscheid

[This page intentionally left blank. ]

**NISTIR 7770**

# **Security Considerations for Remote Electronic UOCAVA Voting**

Nelson Hastings  
Rene Peralta  
Stefan Popoveniuc  
Andrew Regenscheid  
*Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930*

February 2011



U.S. Department of Commerce  
*Gary Locke, Secretary*

National Institute of Standards and Technology  
*Patrick D. Gallagher, Director*

[This page intentionally left blank. ]

This document has been prepared by the National Institute of Standards and Technology (NIST) and describes research in support military and overseas voting for the Election Assistance Commission and the Technical Guidelines Development Committee. It does not represent a consensus view or recommendation from NIST, nor does it represent any policy positions of NIST.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by organizations even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, organizations may wish to closely follow the development of these new publications by NIST.



## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
1.1	PURPOSE AND SCOPE.....	2
1.2	INTENDED AUDIENCE.....	2
1.3	ORGANIZATION.....	2
<b>2</b>	<b>GENERAL ARCHITECTURE.....</b>	<b>4</b>
2.1	SYSTEM COMPONENTS .....	4
2.2	AUTHORIZED USERS.....	7
2.3	THREAT SOURCES.....	8
<b>3</b>	<b>OVERVIEW .....</b>	<b>12</b>
<b>4</b>	<b>CONFIDENTIALITY .....</b>	<b>14</b>
4.1	POTENTIAL BENEFITS.....	14
4.2	PROPERTIES .....	15
4.3	THREATS TO CONFIDENTIALITY.....	17
4.4	CURRENT AND EMERGING TECHNICAL APPROACHES.....	19
4.5	OPEN ISSUES.....	22
<b>5</b>	<b>INTEGRITY.....</b>	<b>23</b>
5.1	POTENTIAL BENEFITS.....	23
5.2	PROPERTIES .....	23
5.3	THREATS TO INTEGRITY .....	27
5.4	CURRENT AND EMERGING TECHNICAL APPROACHES.....	30
5.5	OPEN ISSUES.....	37
<b>6</b>	<b>AVAILABILITY.....</b>	<b>38</b>
6.1	POTENTIAL BENEFITS.....	38
6.2	PROPERTIES .....	39
6.3	THREATS TO AVAILABILITY.....	40
6.4	CURRENT AND EMERGING TECHNICAL APPROACHES.....	42
6.5	OPEN ISSUES.....	45
<b>7</b>	<b>IDENTIFICATION AND AUTHENTICATION.....</b>	<b>46</b>
7.1	POTENTIAL BENEFITS.....	46
7.2	PROPERTIES .....	47
7.3	THREATS TO IDENTIFICATION AND AUTHENTICATION .....	49
7.4	CURRENT AND EMERGING TECHNICAL APPROACHES.....	53
7.5	OPEN ISSUES .....	57
<b>8</b>	<b>CONCLUSIONS .....</b>	<b>59</b>
	<b>REFERENCES.....</b>	<b>60</b>

This page intentionally left blank.]

## 1 Introduction

The Election Assistance Commission (EAC) requested that the National Institute of Standards and Technology (NIST) research technologies to improve uniformed and overseas United States citizens' ability to vote, as required by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) [1]. Additionally, the Help America Vote Act of 2002 (HAVA) requires the Technical Guidelines Development Committee, with technical support from NIST, to study remote access voting, including voting over the Internet [2]. This report contains the results of NIST's research into threats and security technologies related to remote electronic voting for overseas and military voters.

In December 2008, NIST released NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems* [3], which documents the threats to UOCAVA voting systems using electronic technologies for all aspects of overseas and military voting. NISTIR 7551 considered the use of postal mail, telephone, fax, electronic mail, and web servers to facilitate transmission of voter registration materials, blank ballots, and cast ballots. It documented threats and potential high-level mitigating security controls associated with each of these methods. The report concluded that threats to the electronic transmission of voter registration materials and blank ballots can be mitigated with the use of procedures and widely deployed security technologies. However, the threats associated with electronic transmission, notably Internet-based transmission, of cast ballots are more serious and challenging to overcome and the report suggested that emerging trends and developments in that area should continue to be studied and monitored.

While NISTIR 7551 looked at a variety of technologies for all aspects of the UOCAVA voting process, this report takes a deeper look specifically at the issues associated with remote electronic voting over the Internet. It identifies and defines desirable security properties of remote electronic voting systems and major threats faced by these systems that could violate those security properties. It also discusses the current technologies that could be used to mitigate some of those threats and open issues that may still need to be addressed.

In August of 2010, the EAC posted their *UOCAVA Pilot Program Testing Requirements* document [6]. This document defines requirements for remote electronic voting systems using a supervised-kiosk architecture that is intended for use in a UOCAVA pilot program. However, this report considers all remote electronic voting systems, with particular attention to the threats and technologies for remote voting from personally owned and operated devices. Depending on how it is used, the supervised kiosk model mitigates

many of the threats identified in this document, particularly those related to software integrity, coercion, vote-selling, and voter identification and authentication.

### **1.1 Purpose and Scope**

On April 26, 2010, the EAC submitted their *Report to Congress on EAC's efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems* [7], detailing a roadmap intended to be used by the EAC, NIST, and the Federal Voting Assistance Program (FVAP) to create and implement guidelines for remote electronic absentee voting systems for overseas and military voters. The initial phase of this roadmap calls for a report describing security issues related to remote electronic absentee voting system for UOCAVA voters. This report, along with NIST's initial report on threats to UOCAVA voting systems, NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems* [3], is intended to meet this need.

This document is part of a series of documents that address the UOCAVA voting. In addition to NISTIR 7551, NIST has released drafts of NISTIR 7682, *Information Systems Security Best Practices for UOCAVA-Supporting Systems* [4] and NISTIR 7711 *Security Best Practices for the Electronic Transmission of UOCAVA Election Materials* [5]. In addition to NIST's research on security issues associated with remote electronic UOCAVA voting, NIST is also researching usability and accessibility topics. A report documenting this research, *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting*, will be released in early 2011.

### **1.2 Intended Audience**

This document is intended for election officials, technologists, advocacy groups, UOCAVA voting system vendors, and other members of the elections community that will be working with the EAC, NIST, and the FVAP on improving the UOCAVA voting process with the use of electronic technologies. While this document assumes familiarity of the UOCAVA voting process and a high-level understanding of information system security technologies, it is intended to be accessible to a wide audience.

### **1.3 Organization**

The remainder of this report is organized as follows:

- **Section 2** provides a high-level description of the remote electronic voting system architectures that are analyzed in the remaining sections this document. The primary architecture considered is remote voting over the Internet from personally-owned devices.
- **Section 3** provides an overview of the structure for the sections containing the subtopics: Confidentiality, Integrity, Availability, and

## Security Considerations for Remote Electronic UOCAVA Voting

Identification and Authentication. Each subtopic contains a discussion of the potential benefits, properties, threats, current and emerging technical approaches and open issues.

- **Section 4** discusses issues related to confidentiality of remote electronic voting systems. Confidentiality refers to the concept of ballot secrecy, and also to protecting sensitive voter information and system data from unauthorized disclosure. This section discusses desirable properties of remote voting systems to deal with confidentiality issues, threats, and possible mitigating technologies.
- **Section 5** discusses issues related to integrity of remote voting systems. This includes data integrity, aimed at safeguarding important election records, including cast ballots and audit logs, as well as software integrity. It describes desirable properties of systems intended to support data and software integrity and identifies threats and possible technical approaches for dealing with these issues.
- **Section 6** describes properties, threats and technologies related to availability of voting systems. Availability refers to the ability of the system to be ready for use when needed by voters and election officials in the face of malicious and incidental threats.
- **Section 7** discusses issues related to the identification and authentication of voters, system operators, election officials, and system components. It identifies threats to the authentication process and discusses various technical methods for authenticating users and components.
- **Section 8** summarizes the important findings report.

## 2 General Architecture

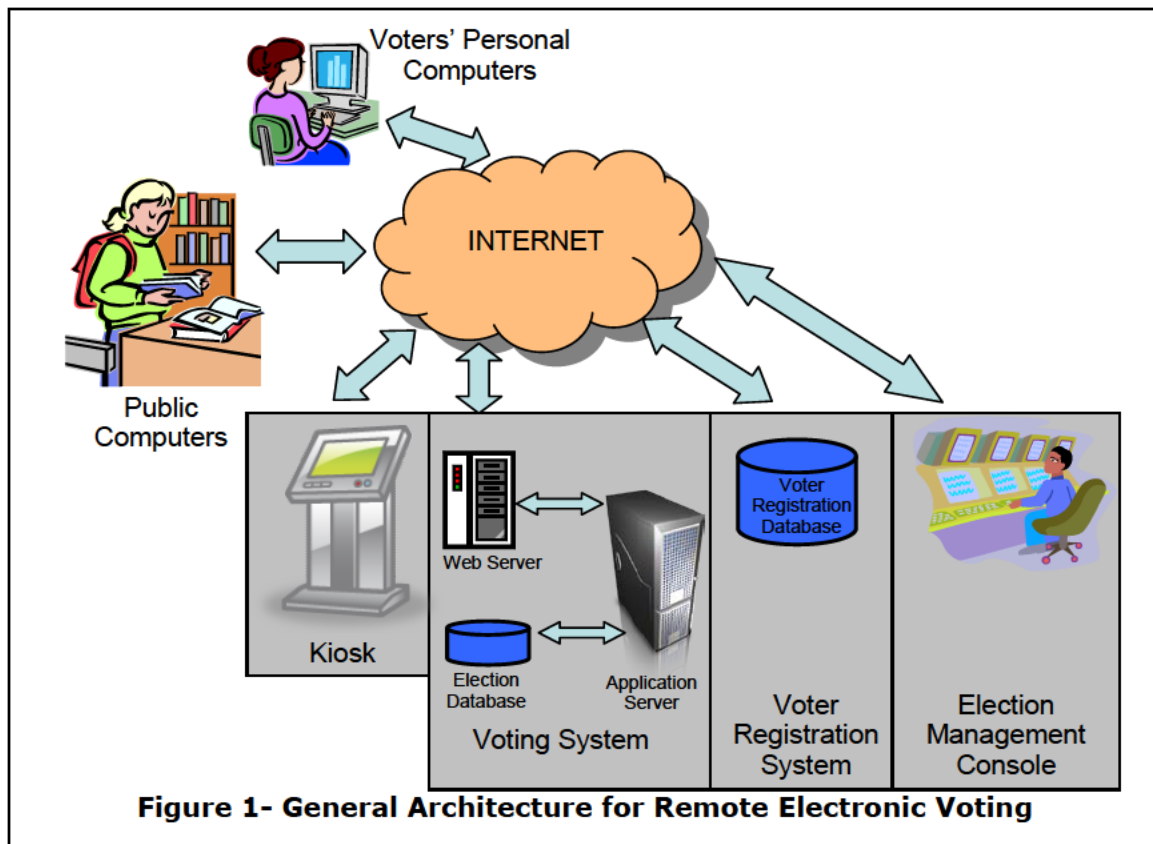
The following section provides an architectural view of remote voting systems in order to provide a reference from which to discuss security considerations presented in the rest of the document.

### 2.1 System Components

The general architecture of electronic remote voting systems, as shown in Figure 1, is composed of several different components. The following subsections detail the components that may be found in an electronic remote voting system.

#### 2.1.1 Voters' Platforms

Figure 1 shows three different platforms that may be used by a voter to request, receive, and cast their ballot: personal computers, public computers, and kiosks.



Personal computers refer to general purpose computing systems a voter may have at home for their personal use, including desktop and laptop computers, tablets, and smart phones. Voters may also use general purpose computer systems found at public locations such as libraries, schools, and Internet cafes and are referred to as public computers. Finally, voters may use dedicated devices called kiosks that may or may not be under the control and supervision of poll workers and/or election officials. In general, the voter's platforms will have a connection to the Internet in order to complete the voting process.

The voter's platform is not under the control of election officials except in a supervised kiosk voting system architecture. This means that there may be no poll worker or election official to ensure the voter's privacy has not been compromised or that voters have not been coerced into casting their ballot differently than they desired. In addition, the platforms not under the control of election officials may be poorly protected and vulnerable to malware, phishing, and denial of service attacks. These platforms may be the target of attacks to monitor and/or modify voter choices, capture personal information, or prevent a voter from accessing the voting services.

### **2.1.2 Voting System**

Figure 1 shows the voting system consisting of three subcomponents: web, database, and application servers. This is a simplified representation of the three subcomponents since they may include other hardware and software not shown in the diagram to ensure system reliability and availability.

The web server provides the interface that voters use to interact with the remote electronic voting system. The web server interface may have the voter use a general purpose browser or a voting-specific client application to obtain voting services from the voting system. The web server has a connection to the Internet so voters can interact with the remote electronic voting system. In addition, the web server will interact with the application server that provides the voting services to the voter.

The application server contains the logic for the services provided by the remote electronic voting system. The services provided by the application server may include the ability for the voter to: register to vote, request a blank ballot, return completed ballots, tally the ballots, and generate election reports. The application server has an indirect connection to the Internet via its interactions with the web server. This provides the voter interface to the remote electronic voting system. In addition to interacting with the web server, the application server will interact with election database and possibly the voter registration system.

The election database contains the ballots for the different jurisdictions serviced by the remote electronic voting system. When a voter requests a ballot, the application server queries the election database to find the appropriate ballot for the voter based on their information. In addition, the election database server may store completed ballots when they are not stored on the application server. The election database server usually does not have a direct connection to the Internet. Access to the database takes place through the application server.

In general, the web server, application server, and election database are housed in one location, such as a data center managed by a jurisdiction or commercial third party. The locations that house the servers and database will need to provide the physical storage space, communication connections, and physical and logical security measures.

### **2.1.3 Voter Registration System**

Voter registration systems are run by states and contain a repository of eligible voters who can participate in elections. The voter registration system assembles the repository of eligible voters using information from different sources such as department of motor vehicle records, judicial records, and possibly the remote electronic voting system. States provide jurisdictions with the registered voter information when elections are held. Jurisdictions can use the information to ensure that only eligible voters are allowed to cast ballots and that only one ballot is cast per voter. Figure 1 shows the voter registration system being accessed directly via an Internet connection or a more limited connection such as a state or military operated network. The jurisdictions may use their connection to the voter registration system to access the voter information in real-time during the election or to make electronic copies of the information they need at a given point during the election.

### **2.1.4 Election Management Console**

Election officials that administer elections use the election management console. The election management console provides an interface to the voting system so administrative task, such as the configuration of ballots, defining the time and date to cast ballots, setting up the tallying rules for the election contests, and the generation of election reports, can be completed. The election management console can be located in the same place as the voting system or may be at some other location (such as the office of the election officials).



### **2.1.5 Component Connectivity**

In general, the components that voters interact with (e.g., voters' personal computers, public computers, and kiosks) use the Internet as their connection to the voting system.

Remote electronic voting system servers and other backend system components may be on the same local network or connected to one another over the Internet.

## **2.2 Authorized Users**

Each of the components of a remote electronic voting system is under the control of one or more different people called users. The users that control the different components are authorized to perform certain, but possibly not all, actions on the component. Although the users are authorized to perform actions on the components, they have the potential to attack the remote election voting system. This section will describe the different users found in the remote electronic voting system but will leave the description of the potential threats which these users present for Section 2.3 Threat Sources.

### **2.2.1 Voters**

The basic voting functionality required by a voter is to: (a) submit voter registration information, (b) request and receive blank ballots, (c) complete a ballot, and (d) return a completed ballot. Voters may use their own personal computers, public computers, and/or kiosks to interface with the remote electronic voting system. In general, voters only have limited capabilities on public computers and kiosks.

Kiosks typically do not have general-purpose applications, such as word processors or email clients, so voters do not have access to these types of applications when voting from a kiosk. However, public computers may provide voters with access to applications other than voting, such as word processors, email clients, and web browsers.

When using their own personal computers, it is the responsibility of the voter to install, configure, and protect their personal computers and the applications that reside on the computer. The different platforms voters use to interface with the voting system have different security and function advantages and disadvantages when considering remote voting system architectures.

### **2.2.2 Election Officials**

Election officials require the capability to administer an election, including adding or removing voters from the voter registration database, configuring ballot styles, defining the time and date to cast ballots, setting up the tallying rules for the election contests, and the generation of election reports. Election officials may interface with the remote electronic voting system via the election management console. As described in Section 2.1.4, the election management console may or may not be co-located with the voting system.

### **2.2.3 System Administrators**

System administrators will require the capability to install, configure, and protect the different components of the remote electronic voting system. In addition, the system administrator will ensure the components they are responsible for can connect to other components of the remote voting system as needed. The system administrator will monitor the components they are responsible for to look for signs the components are operating improperly or are under attack. The system administrator will vary from component to component. Depending on how the architecture is implemented, third party service providers may make up the system administrator for all the components except for the voter's personal computers. Voters are the system administrators for their personal computers. Election staff will serve as system administrators for the kiosk, voting system, voter registration system, and election management console.

### **2.2.4 Auditors / observers**

Auditors and observers will need access to information generated or observed during an election in order to perform their functions. In general, auditors and observers will have limited information collected through observation due to the distributed nature of remote electronic voting systems. Most of the information auditors and observers will have access to will be electronically generated by the remote electronic voting system with a possible exception when paper ballots are used or a voter verified paper audit trail is produced. The integrity and accuracy of the information used by the auditors and observers will greatly impact the effectiveness of their functions.

## **2.3 Threat Sources**

Threat sources are groups or individuals that could feasibly attack a voting system. Some attacks on voting systems could be conducted by almost any dedicated individual, while others may require significant resources, knowledge or access to voting system equipment. Threat sources can be

broken down into two classes: internal and external sources. Internal sources are individuals or groups with some level of authorized access to the voting system equipment or the supporting infrastructure (e.g. the communications network). External sources are individuals or groups that do not have any special level of authorized access to the voting system equipment or supporting infrastructure. This report considers the following examples of threat sources.

### **2.3.1 Internal Threat Sources**

In general, internal threats come from individuals or organizations with privileged and authorized access to the remote electronic voting system required to support or carry out use of the system in an election. Threats from inside sources may be more dangerous and more difficult to protect against since they have some level of access to the system.

**Voters:** Voters' access to the remote electronic voting system is limited through the voters' platform used: their own personal computers, public computers, and kiosks. In general, voters will not have direct access to the voting system, voter registration system, or election management console. Voters are allowed to submit voter register information, request and receive blank ballots, complete a ballot, and return a single completed ballot. However, voters may use their voting platform to try to cast multiple ballots using multiple credentials, prove how they voted to sell their vote, expand their access to damage the voting system, change the results of the election, or harm the credibility of the election results.

In addition, the voting platforms may pose a threat to the remote electronic voting system without the voters' knowledge or cooperation. When voting platforms contain malware, the voting platform may try to inhibit a voter from casting his or her ballot, alter a voter's choices, monitor how a voter votes, use the voter's credential to gain and expand access to damage the voting system, change election results, or harm the credibility of the election results. Although the voter is not actively participating in attacking the remote electronic voting system, the platform they use to interact with the voting system poses a threat that appears to be from the voter.

**Election Officials:** Election officials access the remote electronic voting system via the election management console and possibly voting system equipment as authorized users on the voting system component. Election officials are allowed to add eligible voters to the voter registration database, remove ineligible voters, configure ballot styles, define the time and date to cast ballots, set up the tallying rules for the election contests, and generate election reports. However, election officials may not need to be able to

install and configure applications or have unrestricted access to the remote electronic voting system equipment. Election officials will have access to election data, such as cast ballots and system event logs, on the remote electronic voting system that most other authorized users may not. Access to the election data may allow a malicious election official to modify the results of the election, monitor how people vote, and provide incorrect ballot configurations.

Similar to the voter and voters' platform, the election official and election management console may pose a threat to the voting system without the election official's knowledge. If the election management console contains malware, the console may try to prevent ballots from being cast, alter ballot configurations, monitor how voters vote, and use the election official's credential to gain and expand access to damage the voting system, change election results, and harm the credibility of the election results. Although the election official is not actively participating in attacking the remote electronic voting system, the console they use to interact with the voting system poses a threat that appears to be from an election official.

**System Administrators:** System administrators access the remote electronic voting system equipment via a remote connection or a terminal directly connected to the equipment. In addition, system administrators have physical access to the equipment. System administrators are allowed to install, configure, and monitor the remote electronic voting system equipment to ensure the equipment is functioning properly. System administrators may directly administer the components of the remote electronic voting system or the supporting infrastructure used by the system. For example, network technicians at telecommunication companies or Internet Service Providers (ISPs) are system administrators of the infrastructure used by the remote electronic voting system. Election IT staff are system administrators for the election management console when it is located at the election official's office. System administrators have a level of access to the system that no other authorized user has in order to configure and maintain the system. Given this level of access, system administrators may try to prevent ballots from being cast, alter ballot configurations, monitor how voters vote, damage the voting system, change election results, or harm the credibility of the election results.

**Other insiders:** There are other internal individuals or organizations that may have access to the remote electronic voting system equipment before, during, or after an election cycle. For example, voting system manufacturers will have access to the software source code and hardware designs used to implement their remote electronic voting system. This level of access provides an opportunity for errors to be introduced, maliciously or not, into

the components of the remote electronic voting system. Voting system integrators have similar access as voting system manufacturers, but without access to the software source code or the designs of hardware components. This level of access provides the opportunity for known software and hardware errors to be exploited, and for third party, non-voting specific software and hardware to be integrated into the remote electronic voting system components containing errors; malicious or not. The support staff of different organizations, including but not limited to jurisdictions, voting system manufacturers, voting system integrator, and third party service providers, may have access to the remote electronic voting system equipment and that provides an opportunity for the system to be exploited. Examples of support staff include administrative assistants, package and mail delivery personnel, and warehouse personnel.

### **2.3.2 External Threat Sources**

In general, external threat sources come from individuals or organizations not needed to support or carry out use of the system in an election.

***Hostile Individuals:*** Individuals and affiliated individuals may attempt to inhibit ballots from being cast, monitor how voters vote, damage the voting system, change election results, and harm the credibility of the election results. These individuals rely on their technical knowledge and ability to deceive legitimate users and administrators. In general, attacks from hostile individuals are limited based on resources – time, money, and people – they can accumulate or control as required for a given attack scenario.

***Hostile Organizations:*** Like hostile individuals, hostile organizations that may not have legitimate access to the remote electronic voting system in order to attempt to inhibit ballots from being cast, monitor how voters vote, damage the voting system, change election results, and harm the credibility of the election results. Hostile organizations can marshal more resources, particularly money and people, to conduct an attack on the remote electronic voting system than an individual. Given these added resources, a hostile organization can recruit, hire, and train individuals, as well as obtain more costly technology to conduct an attack on the system. Hostile organizations can take many forms including civilian, foreign-sponsored, or terrorist organizations.

### 3 Overview

The remainder of this report discusses security issues that need to be considered when developing, deploying, or using remote electronic voting systems. The discussion divides the issues into four topic areas:

- **Confidentiality:** Confidentiality refers to the concept of ballot secrecy and also the protection of sensitive voter information and system data from unauthorized disclosure. Issues related to confidentiality are discussed in Section 4.
- **Integrity:** This includes data integrity, aimed at preventing important election records, including audit logs and cast votes, from being improperly modified, as well as software integrity. Issues related to voting system integrity are discussed in Section 5.
- **Availability:** Availability refers to the ability of the system to be accessible to voters and election officials in the face of malicious and incidental threats. Issues related to voting system availability are discussed in Section 6.
- **Identification and Authentication:** Identification and authentication includes the identification and authentication of voters, system operators, election officials, and system components. Issues related to the identification and authentication of voting system users and components are discussed in Section 7.

These areas were chosen to break the discussion of security issues into closely related topic areas. Issues related to any one of these topic areas are closely bound to those associated with other topics. For instance, an insufficient authentication mechanism could allow an unauthorized individual to access sensitive information (a confidentiality violation) or modify key voting system records (an integrity violation).

For each topic area, this report discusses the following:

- **Potential Benefits:** The move from the current mail-in absentee voting process to a remote electronic voting system can provide some benefits to security, such as in the areas of automated forms of strong authentication, timeliness of delivery, and ballot secrecy. For each of the topic areas, this report will describe the advantages of remote electronic voting.

## Security Considerations for Remote Electronic UOCAVA Voting

- **Properties:** In order to facilitate discussion of threats to remote electronic voting systems, this report provides lists of desirable security properties. In general, threats identified in this report are actions that can violate one or more of those properties. The security properties identified in this report are based on properties and requirements identified in other electronic remote voting system documents including the Secure Electronic Registration and Voting Experiment (SERVE) Project documentation [10], the Common Criteria Protection Profile for online voting systems [8], and the Council of Europe's standards for online voting systems [9]. Policymakers ultimately must decide which properties must be met by voting systems to be acceptable in their jurisdictions. This report provides notes with each property that can help policymakers decide which properties are realistically achievable with current and emerging security technologies.

This report provides definitions for the identified desirable security properties. While definitions may be written in absolutes, readers should recognize there are always tradeoffs that have to be made. For example, the extent a security property can be met versus the cost and usability of implementing the property. Acceptable tradeoffs must be made when deploying systems which often necessitates compromising strict interpretations of some of the proposed properties.

- **Threats:** This report describes some of the major threats to remote electronic voting systems. However, this document is not intended to be a thorough threat or risk assessment on remote electronic voting systems. This document describes some of the more serious threats to remote electronic voting systems. It does not attempt to enumerate all threats. Readers should consult other resources, such as NISTIR 7551, for information on additional threats.
- **Current and Emerging Technical Approaches:** This report identifies and describes some existing and emerging technologies that can be used to mitigate some of threats faced by remote electronic voting systems.
- **Open Issues:** Some security issues associated with remote electronic voting do not have complete solutions at this time. In some instances, advances in technology are needed to address threats, while in other cases the technology is developed, but is not widely deployed.

## 4 Confidentiality

Voting systems must protect the confidentiality of sensitive information stored on those systems. Notably, remote electronic voting systems have unique concerns about protecting ballot secrecy compared to polling place systems. While an electronic voting machine in a polling place typically does not learn the identities of voters interacting with it, remote electronic voting systems typically must identify and authenticate voters in order to verify their eligibility and provide them with the proper ballots. In some jurisdictions, local or state election procedures dictate that the identities of overseas and military voters must be able to be linked to cast ballots, a property usually forbidden in polling place systems. Despite this, remote voting systems must protect their information from being used illegitimately.

Remote electronic voting systems must also protect the confidentiality of other sensitive information on those voting systems. Remote electronic voting systems may include an online voter registration database containing sensitive personally identifiable information. They must also protect sensitive system information that could be used to compromise the security of the system, such as secret cryptographic keys or passwords.

### **4.1 Potential Benefits**

Compared to mail-in voting, remote electronic voting systems have the potential to provide much greater technical controls for maintaining ballot secrecy. With mail-in voting, ballot secrecy is protected by procedural means: identities of voters are physically separated from cast ballots prior to viewing the contents of the ballots. Small-scale ballot secrecy violations are still possible if colluding election workers handling mail-in ballots do not follow proper election procedures. Access control mechanisms and cryptographic technologies can provide strong protections against attacks on ballot secrecy. Technical measures can be taken so an arbitrarily large number of trusted officials must collude to violate ballot secrecy.

Furthermore, remote electronic voting systems can also provide some protection against unsophisticated attempts to coerce voters. For instance, systems may allow voters to cast multiple ballots and only count the final ballot issued by the voter. If voters feel pressure to vote a particular way in one instance, they would be able to cast a new ballot at some other time or location free from improper influence. While it is significantly more difficult to block coercion attempts from more sophisticated or determined attackers, this is still a useful benefit offered by remote electronic voting systems.



## 4.2 Properties

This section discusses high-level properties aimed at assuring confidentiality of the vote and of the voter. Confidentiality is necessary to protect the autonomy and privacy of the voter as well as the secrecy of the vote.

A strong form of enforced confidentiality, called receipt-freeness, is also discussed. This property makes it impossible for the voter to prove to a third party how he or she voted. This property addresses the threats of coercion and buying/selling of votes.

### Property: Ballot Secrecy

*The voting system protects the secrecy of cast ballots.*

#### Notes:

All voting systems leak some information about voters' choices. Such information can usually be derived from data made public during the election (e.g., partial tallies, lists of voters). The remote electronic voting system should not add to this loss of secrecy in any meaningful way. In particular, a voter should not lose plausible deniability regarding his or her vote. Protecting ballot secrecy does not necessarily mean that it must be impossible to link individuals to cast ballots; state law regarding ballot secrecy differs from jurisdiction to jurisdiction. While the general public should not be able to perform this linkage, election officials acting in accordance with state and local election law and procedures may be required to have the capability to link voters to cast ballot. For these cases, voting systems should implement protections to ensure that ballot secrecy can only be breached when proper procedures are followed. For example, the system could force multiple trusted election officials to jointly interact with the system to violate ballot secrecy, and the system could only provide mechanisms for linking single ballots, not all ballots at once.

### Property: Protection of Personal Information

*The voting system protects voters' personal information from unauthorized disclosure.*

#### Notes:

The voting system should not needlessly store voters' personal information. Any personal information that is stored should be protected against unauthorized disclosure. Use of encrypted storage is recommended in order to minimize the damage caused if storage media is lost or stolen, and access control mechanisms should be used to limit access to sensitive information.

**Property: Receipt-freeness**

*Voters are not able to provide convincing evidence of their ballot selections to third parties.*

**Notes:**

The threat of vote selling and coercion attacks becomes more serious if voters are able to give attackers evidence of how they voted. This information could be used to reward the voter for voting correctly in a vote-selling attack or as evidence that the voter met the demands of a coercer.

Notably, remote voting systems should not increase the likelihood of large-scale buying and selling of votes compared to current mail-in voting methods. They also should not increase the likelihood of large-scale coercion of voters. Coercion is different from vote buying in that the voter is not a willing participant.

**Property: Protecting sensitive system data from improper disclosure or use**

*All sensitive system information handled by the voting system should only be readable by authorized administrators or election officials.*

**Notes:**

Examples of sensitive system data are: passwords or keys used by the election officials to access, configure, and run the voting system; and timestamps recording when voters authenticated or cast ballots.

**Property: Minimal storage**

*The voting system only stores sensitive information necessary to ensure the correct functioning of the voting system.*

**Notes:**

While there are many safeguards that can be put in place, online systems are at risk for unintended data breaches. Internet-accessible systems should not store sensitive information that is not needed by the system. Notably, voter registration databases may contain sensitive voter information, such as identification numbers, that may not be needed by the voting system. When the voting system operates its own voter list or database, sensitive data fields should not be copied over from the primary voter registration database unless the information will be used by the voting system.

**Property: Limited communication**

*Only necessary communications traffic is passed between entities participating in the voting process.*

**Notes:**

As a general rule, there should be limited communications between voting system components. Passing extraneous information, even information that may look benign, increases the chance that this information could be combined to violate confidentiality goals, such as ballot secrecy.

**4.3 Threats to Confidentiality**

This section discusses some of the more significant threats to confidentiality that are either unique to remote electronic voting systems or that may be more severe in this context. This is a high-level classification that addresses generic threats for all remote voting systems. It does not address threats to individual voting system implementations.

**4.3.1 Central System Data Breaches**

A data breach is an unintentional release of secure information to an unauthorized party. In the context of voting systems, data breaches can cause loss of vote secrecy as well as loss of private voter information. The potential damage of private information exposure may be less severe in voting systems than in some other systems, such as financial databases or health databases, since voting systems do not need to store as much sensitive private information.

Storage of unencrypted sensitive information carries increased risk and should be avoided when possible. Connection to the Internet also increases the risk of a data breach. Failure to properly secure encryption keys and passwords can result in granting unauthorized access to malicious (or simply curious) third parties. Poor key management can result in insufficiently vetted personnel (e.g., temporary workers) obtaining decryption keys that they are not supposed to have. This can lead to serious data breaches. Additionally, compromised keys can harm the integrity of stored or in-transit data.

A remote electronic voting system may use an external database (e.g., a vehicle registration database). In this case, the voting system could become a route for exposure of private information contained in the external database. Standard database security practices should prevent sensitive information from being exposed. However, the scenario in which two

database administrators each assumes the other is responsible for preventing data breaches is a concern.

### **4.3.2 Coercion**

Voting systems that allow the voter to vote more than once can make it harder to effectively coerce voters (since voters could vote again at a later time). On the other hand, if the secrecy of the vote is not secured, then coercion can be a more serious problem than in non-electronic voting. The reason is that electronic coercion attacks can scale easier and impact more voters and ballots. In particular, coercion that takes the form of reprisals long after the election has ended could be a serious problem, should the secrecy of the vote be compromised on a broad scale. If the voting system has a capacity to link cast ballots to voters (say, under a court order or a voter challenge), then it may be desirable to implement a mechanism for permanent removal of this capacity. In principle, this would occur via destruction of secret keys after a prescribed amount of time has elapsed. Keys that are meant to be eventually destroyed could be split into electronic components and tamper-evident physical components to help ensure the keys are destroyed. In modern information systems, it is very difficult to fully ensure the destruction of electronic data.

### **4.3.3 Buying and Selling of Votes**

A concern with remote electronic voting is the possibility of a market for voting credentials could emerge. A similar threat exists in the case of mail-in voting, in which the unfilled ballots could be bought and sold. However, the scalability and increased anonymity inherent to remote electronic voting potentially makes this a more serious concern. We do not know how to gauge the likelihood of this threat in the presence of law-enforcement deterrents. We note that, in most cases, this threat requires the willingness of both buyer and seller to commit a crime. This should serve as a significant deterrent to vote selling for most of the voting population. On the other hand, any change in voting technology implies a corresponding change in the cost/benefit equations that determine the extent of illegal practices such as vote selling.

A related concern is vote swapping (i.e., vote pairing). This occurred in the 2000 and 2004 elections in the US. It is conceivable that the deployment of Internet voting could cause a surge in this practice if there is an easy mechanism to exchange credentials to voting systems or verify how individuals voted.

Since long-lived voter credentials may increase the likelihood of these types of threat, it may be advantageous to have voters obtain at least part of their voting credentials in the days or weeks prior to the election.

#### **4.3.4 Malicious Software on Client Systems**

An emerging threat to computer systems over the last few years is that of malicious software infecting computers, giving attackers control of these systems. Researchers from the Georgia Tech Information Security Center have estimated that attackers may control 15 percent of online computers in this way [12]. What "control" means here is that the machines have been infected by malware that allows some level of access to them. The level of access is typically enough to steal private information and tap communications. Compromised machines could potentially violate the secrecy of the vote. Votes could be linked to machines or, depending on the voting protocol, even to voter identities. While this is clearly illegal, it is unclear what value this information might be to criminals. Unlike credit card numbers, there is no clear financial gain from knowing how a person voted. This is particularly true if such knowledge cannot be verified by a third party (as anyone can claim to know how someone else voted). Furthermore, this type of information is typically only valuable in bulk (as a reference, a single stolen piece of credit card information sells for between \$0.85 to \$30 [14]). Bulk voting information has two principal uses: tying demographics to voting and large-scale voting coercion. The former is easily obtainable from statistical analysis. The latter seems to be a low-likelihood threat on two accounts: i) it necessitates verifiable information; and ii) it appears hard to do without getting caught.

If compromised machines are able to steal verifiable voting information, then another threat scenario is plausible: vote buying and selling. Opinions vary regarding the severity of the vote buying and selling threat.

### ***4.4 Current and Emerging Technical Approaches***

This section discusses the main tools at our disposal for secure implementation of remote electronic voting systems. Some of the tools are standard IT security mechanisms, whereas others are of special applicability to voting.

#### **4.4.1 Cryptographic Protections**

Cryptography can protect any data that is communicated from one system to another as well as stored data. For example, the data which travels through the Internet between the voting system and the voter's computer can be efficiently protected from unauthorized access via protocols like

Secure Socket Layer (SSL) or Transport Layer Security (TLS) [15]. SSL and TLS are widely-deployed encryption mechanisms that are often used to protect communications between a web server and browsers. When used with mutual authentication, these protocols provide end-to-end security.

When used to protect data at-rest, cryptographic keys can be split between several people, requiring an arbitrary number of key holders to come together to decrypt data. Such mechanisms offer protection against insider attacks, as long as a small number of insiders can be trusted to not collude in an attack.

Proper cryptographic key management is very important to achieving protection using cryptographic techniques. Keys must be generated, stored, used, and destroyed in specific ways to ensure there are not ways to bypass the cryptographic protections.

#### **4.4.2 Advanced Cryptographic Voting Techniques**

Modern cryptology provides several possible solutions for securely conducting secret-vote online elections. These solutions provide very good properties in idealized scenarios where voters make no mistakes, have complete control of their computers, and communication lines are reliable. The scenarios typically allow for fraudulent voters attempting to sabotage the election and for attackers having unimpeded read access to all communication lines. The result of these idealized protocols is that a tally of the votes of all honest voters is obtained and is publically verifiable without compromising the secrecy of the votes.

Despite there being an abundance of voting protocols with the above properties ([16][17][18][19][20] are just a few), the problem of remote voting using the Internet is far from solved. This is because the Internet is not the idealized scenario assumed by that body of work. Voters make mistakes and their computers may be partially under the control of malware. Communication lines may not be reliable. Also, there have been no formal usability or accessibility studies of current cryptographic voting schemes yet, but researchers anticipate that such studies would identify issues that would need to be addressed. Further research may lead to dramatic improvements, but current cryptographic voting techniques do not solve many of the challenges associated with remote electronic voting.

#### **4.4.3 Access Control Mechanisms**

Access control mechanisms can be used, in conjunction with identification and authentication mechanisms, to restrict access to data, applications or

actions to particular users. Different levels of access can be granted to different users; a relatively common set of access levels include read, write, and execute permissions, and modern access control mechanisms often provide more fine grain control over permissions. Access control can be implemented in many different ways. On computer systems, access control mechanisms are most often enforced by operating systems, and, in the case of voting systems, voting applications.

For example, access control mechanisms could provide only a designated election official with the access rights to write, modify or delete ballot definition files, but give a much wider set of users access rights to only read those files.

Access control mechanisms could also implement things such as dual-person control, whereby the system requires two or more users to authenticate to the system before providing access to a particular resource. However, such functionality is often not provided by modern operating systems or applications. When used, dual-person control is often implemented with a combination of technical and procedural means.

Depending on how access control mechanisms are implemented, it may be possible to bypass those protection mechanisms. For example, if access control mechanisms are enforced by an application, users may still be able to access resources through the operating system. If the operating system enforces access control mechanisms, an individual with physical access to the system may be able to access resources by booting from a different operating system. Furthermore, in many modern operating systems, the system administrator, or root user, often has nearly unlimited control over the system. For these reasons, it is important to also use cryptographic protections to restrict access to sensitive data, rather than solely relying on common operating system or application-level access control mechanisms.

#### **4.4.4 Separation of Duties**

With a combination of procedural and technical means, operators of remote voting systems can enforce separation of duties to limit the capabilities of any single user or computer system. For instance, important information or tasks could be split between several election officials or system operators, requiring them to collude to conduct an attack. One example of how this could be implemented is that one official could be given a key to a locked room with voting system equipment, while a second official is given a credential for administering the voting system equipment.

## ***4.5 Open Issues***

Achieving a very strict notion of ballot secrecy remains a challenging issue in remote electronic voting systems. While polling place voting systems do not store, or even learn, the identities of voters, remote electronic voting systems need to authenticate voters before allowing them to cast ballots. Cryptographic protocols exist to protect the secrecy of ballots even from those with unrestricted access to voting system equipment, but these technologies may not be ready for immediate use with remote electronic voting systems. For technical, procedural, and legal reasons, it is likely that any deployed voting system for UOCAVA voters would still have access to, and probably store, sufficient information to violate ballot secrecy. Depending on policy decisions at state and local levels, this issue may not require a technical solution beyond what is already practical.

Advanced voting-specific cryptographic protocols have highly desirable properties in idealized models, but in practice, systems based on these protocols are often difficult to use and require that cryptographic keys be distributed to voters before an election. These systems also do not protect against many types of attacks, particularly if the computer used to cast votes and the voting environment are not secured.

Current techniques for remote electronic voting do not solve the problems of coercion and vote selling that are inherent to unsupervised voting. Variations on these attacks are possible with mail-in absentee voting, although in that voting method, it is difficult for a single individual to impact many voters. When moving to remote electronic voting, election officials and technologists should consider whether the move makes it easier to scale these attacks. In particular, there appear to be ways that attackers could coerce or buy votes remotely. A simple attack involves selling or transferring the credentials that voters use to log into the remote voting system. This particular issue and threat will be discussed further in the Identification and Authentication section (Section 7).

Despite IT professionals' and users' best efforts, data breaches continue to occur, releasing personally identifiable information (and other sensitive information) to attackers. This problem is not unique to voting systems. For the time being, it may be impossible to guarantee the secrecy of voter information stored on voting system equipment from determined and technically sophisticated attackers. However, there appears to be very little reason to store potentially valuable sensitive information on these systems. Depending on the type of information stored by the voting system, there may be very little motivation to attempt to illegitimately access this information.



## 5 Integrity

This section discusses security issues associated with voting system integrity. Integrity refers to the trustworthiness of the system, including both the data on the system and the functions provided by the system's software. Maintaining integrity involves implementing safeguards to ensure data and software on a system are not modified by unauthorized parties. It is typically preferable to have these safeguards block unauthorized attempts to modify data or software, but in some cases, it is only possible to detect integrity violations.

Integrity includes the concept of the origin or source from which the integrity is based upon. In other words, the origin or source of the integrity for data or software functionality can be traced back to a particular trusted authoritative entity. Tracing integrity back to a particular entity is closely related to identification and authentication, which is covered in Section 7.

### **5.1 Potential Benefits**

#### **5.1.1 Authenticity of Electronic Records**

A cryptographically signed record of each cast ballot can be issued by the voting system components and transmitted for tallying and auditing purposes. The signed record can be easily and exactly replicated to reduce the likelihood of data loss. Assuming adequate key management, the signed record cannot be forged. Authenticity can be verified using public key cryptography.

#### **5.1.2 Strong Integrity Protections In-Transit**

It is a common misconception that the greatest threat associated with conducting transactions over the Internet is the modification of information as it is being transmitted. While this is a potential threat that must be mitigated, in fact there are very good technical solutions for protecting information during transmission. Cryptographic protocols, such as TLS or Internet Protocol Security (IPSec), are very effective at providing integrity protection in-transit.

### **5.2 Properties**

There are two main categories of properties for integrity: data integrity and software integrity. Data integrity is related to the integrity of the election records, especially those records directly used to derive the final election tallies, as well as those necessary for meaningful audits. Software integrity refers to the correct, unmodified software running on the electronic

components of the voting system. Faulty or malicious software may directly affect election data integrity.

### 5.2.1 Data Integrity Properties

#### **Property: Accuracy**

*The election outcome properly reflects the choices of participating voters.*

*Notes:*

The voting system must: (a) record votes consistent with voters' selections, (b) accurately store the collection of cast ballots, (c) protect the cast ballots from unauthorized modification, deletion or insertion, and (d) accurately count the votes.

#### **Property: Auditability**

*The voting system provides evidence of its behavior before, during and after an election.*

*Notes:*

It is not enough for a voting system to merely function correctly. The voting system must also provide evidence to auditors that the system functioned in the way it was supposed to. The evidence could include system event logs, public voting system reports, voter-verified records, and, in some cases, mathematical proofs. In addition, the voting system and its supporting election procedures must provide assurances that the evidence provided by the system is trustworthy. Auditability is a high-level security property of a voting system with more specific sub-properties listed and described in this sub-section.

#### **Property: Privileged verifiability**

*The voting system provides evidence that allows the election auditors to independently check the outcome of the election.*

*Notes:*

In general, verifiability is a voting system property where an observer is able to check the election outcome produced by the voting system is correct. That is, the system should produce ample evidence allowing auditors to verify the results of an election. In the case of privileged verifiability, the evidence provided could be secret or sensitive information that could only be made available to, or authenticated by, election insiders.

**Property: Public verifiability**

*The voting system provides evidence that allows the general public to independently check the outcome of the election.*

**Notes:**

Public verifiability is a property offered by emerging cryptographic voting protocols. In this case, sufficient evidence is made publically available by the voting system so any individual can verify the outcome of the election. Generally this requires some assumptions about the behavior of other entities (e.g., other voters, poll workers, administrators, etc.).

**Property: Traceability**

*The voting system maintains all the necessary information so that if a problem is found in a particular election, then it is possible for the election officials to trace the problem to one or more root causes.*

**Notes:**

If there are any problems during an election, it is important to be able to trace problems back to their root causes. The voting system should log or otherwise track sufficient events on the voting system to determine which activities failed or succeeded.

**Property: Recoverability**

*The voting system maintains necessary information to allow it to recover from a loss of integrity. If the integrity of election records is lost in a way that is irrecoverable, then the extent to which the problem affects the final tally is measurable.*

**Notes:**

If a voting system fails, then it should fail in a graceful manner. A minor problem should not necessarily call into question the integrity of the entire election. When possible, the voting system should be able to recover from minor problems. In some instances a voting system will not be able to recover from an error. In these instances, it should be possible to measure the extent of a failure so appropriate remediation can be carried out.

**Property: Prevention of data alteration**

*The voting system prevents the unauthorized modification, deletion or insertion of election or voting system records.*

**Notes:**

A voting system contains a great deal of data (e.g., system files, election records, and event logs) that must be protected from

## Security Considerations for Remote Electronic UOCAVA Voting

unauthorized manipulation. To the extent possible, the voting system should prevent unauthorized manipulation and detect any manipulation that takes place.

**Property: Logging data alteration**

*The voting system keeps a secure log with the information about who created/modified/deleted data which may influence the outcome of the election.*

*Notes:*

Secure audit logs can help to increase accountability of system administrators and other insiders with privileged access to the machine. The log should be secure against modification by anyone, and should only be readable by authorized users.

**Property: Data authenticity**

*Election auditors are able to verify the authenticity and provenance of election records.*

*Notes:*

While protecting ballot secrecy, the voting system should provide sufficient evidence to allow election auditors to determine what entity (e.g., voter, system administrator, voting system component) created an election record and to verify that the record was not modified by unauthorized parties.

## 5.2.2 Software Integrity Properties

**Property: Integrity of server software**

*Voting system components only load and execute authorized software.*

*Notes:*

The voting system back-end components, such as servers, databases, and supporting network components, should only run authorized software. Front-end components under the control of election officials, such as kiosks, should also only run authorized software. For instance, the system should be free of malicious software. In addition, processes should be put in place to validate and authorize updates to voting system application software other third-party software used on the systems (e.g., operating systems, database software, anti-malware software).

**Property: Authenticity of server software**

*Election auditors and/or system administrators are able to verify that only authorized software is present on voting system components.*

**Notes:**

Auditors and system administrators should be able to verify that the voting system is free of malicious software and that only the authorized software is present on the voting system. In general, software validation is difficult to do rigorously and letting the voting system software verify itself is not sufficient.

**Property: Proper software engineering practices**

*The voting system software is designed, implemented, tested and deployed with accepted software engineering best practices.*

**Notes:**

Software engineering and testing best practices help to reduce errors in the design and implementation of voting systems.

**5.3 Threats to Integrity**

In general, any electronic system is prone to software bugs and malicious software attacks. Bugs and attacks related to software may result in partial loss of data integrity, and thus directly influence the election results. Moreover, Internet voting uses personally owned and operated devices which may be highly vulnerable to attacks that are capable of impacting election integrity. The election officials may have no practical way to assess the integrity of personal computers.

**5.3.1 Software Bugs**

One of the greatest threats to the integrity and accuracy of election records, including cast ballots, comes from non-malicious software defects, called software bugs. Software bugs accidentally written into voting system application software, third-party libraries, and commercial software required to run the voting system all have the potential to impact election integrity.

Software bugs should be expected when dealing with software. In general, the larger a piece of software is, the more bugs are likely present. Estimates on the software industry's rate of bugs range from about 15 to 50 errors per 1000 lines of code [11]. Modern voting system application software can be quite large containing tens of thousands of lines of code. In most cases, voting systems run on top of commercial operating systems which can have

tens of millions of lines of code and use various other commercial libraries of software applications of varying complexity.

Extensive testing and analysis can identify many bugs but will never uncover all of them. Software bugs occur in medical devices, military equipment, and space exploration vehicles, despite extensive and sophisticated testing in these areas. In addition, software bugs affecting cast votes have been identified in certified voting systems [12], despite testing and code review during testing.

Even software whose source code is freely available to the public can contain major software bugs for years without discovery. The OpenSSL library included with the Debian-based linux distributions included a software bug in the cryptographic key generation function that resulted in a serious vulnerability in applications that relied on this library [13]. The bug went unnoticed for more than one year before being patched.

### **5.3.2 Malicious Software on System Servers**

Specialized software could be maliciously placed on voting system equipment to modify or incorrectly store election records. The malicious code could be placed on the voting system equipment at any time in the system's life cycle. Developers of the voting system software, or any software used by the voting system, could include malicious code. Election insiders, such as system administrators, could install malicious software that changes election data. Or, remote attackers may be able to exploit a vulnerability in the voting system to install malicious code on the system. These attacks have the potential to change a large number of votes and can be difficult to detect.

### **5.3.3 Modification of Election Records and Data**

Rather than installing malicious code on voting system servers and other back-end components, attackers may be able to modify election records directly to compromise election integrity. For example, a system administrator may be able to modify records stored on a database server. Or, vulnerabilities in the voting system may allow a remote attacker to perform an SQL injection attack to modify records in the database.

### **5.3.4 Malicious Software on Client Systems**

The threats described in the previous sections are largely variations on similar threats faced by polling place electronic voting systems. However, Internet voting systems are also faced with threats to voters' personal

## Security Considerations for Remote Electronic UOCAVA Voting

computers which are used as voting terminals. Attacks on these systems fall into a category generally referred to as client-side attacks. In most cases, these involve an attacker infecting a victim's computer with malicious software (e.g., a computer virus, trojan or worm) in order to gain access to information stored on that client machine or control it in various ways.

Client machines are quickly becoming a predominant attack vector in all types of information technology systems. Given the amount of sensitive information often stored on web, file, and database servers, these servers are often very tempting targets for attacks but they also tend to be the best protected, with professionally trained system administrators configuring and monitoring those systems. Client machines, used by regular employees or individuals, are often much less protected against attacks since they are operated by less technically sophisticated users. The client machine may be the intended target of an attacker, or it may be used as a stepping stone to attacking another computer system.

Attacks can use a variety of means to get malicious software on individuals' personal computers. Historically, file attachments sent over electronic mail were a common method for distributing malicious software. Alternatively, an attacker could post malicious software that appears to have a desirable purpose (e.g., a game, anti-virus software, screensaver, etc.) on a web site and encourage people to download it. In these cases, the victim became infected with the malicious software by executing the file attachment or downloaded file.

More recently, vulnerabilities in commonly used software became a common attack vector for malicious software. Some malicious software is self-replicating, where infected machines seek out other machines to infect, such as the 2003 Blaster worm that exploited a vulnerability in the Windows operating system. Individuals could become infected with the Blaster worm merely by connecting their Windows computer to the Internet. New vulnerabilities in commonly used application software have led to a new attack method, commonly referred to as drive-by-downloads. Using vulnerabilities in browsers, browser plugins, and other commonly used software, users can become infected with malicious software merely by visiting infected web sites.

An infected machine is largely under the control of an attacker. If a voter's personal computer becomes infected with a malicious software targeting the election, an attacker can potentially steal the victim's authentication credentials (e.g., a password or PIN), or even change the victim's vote without the victim noticing.

Malicious software is a serious problem on the Internet, with a large number of computers already infected with some type of virus or trojan. A growing problem on the Internet is botnets: groups of infected computers under the control of an attacker. The malicious software running on infected computers in a botnet is often used to steal passwords and other credentials for email and social networking sites in order to facilitate spreading the software to other computers. In many cases, the purpose of the attack is to steal financial data, such as passwords to online banking sites or credit card numbers. In some cases, malicious software on botnet-infected computers can even change the data inputted on a website for a financial transaction. For instance, it can change the bank account destination and amount for a money transfer on an online banking website.

Botnets are sometimes rented or sold by the individuals that originally conducted the attack to other parties. In addition, the malicious software behind the botnets is sold on black-market websites. For example, the malicious software behind the Zeus botnet is sold for as little as \$700. Researchers at Cisco found that attackers could build a complete Zeus botnet for \$2500, which includes the cost for the Zeus malware, exploit tools to infect users, and servers for conducting the attack [22]. While existing malicious software would have to be modified to attack an Internet voting system, this may not be difficult. In fact, many existing botnets include the ability to remotely update the malicious software running on already-infected computers. This means attackers would not necessarily have to re-infect computers already in botnets to attack an Internet voting system.

Because voters' personal computers are outside the control of election officials and voting system administrators, client-side attacks are very difficult to mitigate. While each successful attack on the client can only impact one vote or voter (or potentially a small number of voters if a computer is shared), attackers have demonstrated an ability to infect a large number of clients, and thus client-side attacks have the ability to have a large-scale impact.

#### ***5.4 Current and Emerging Technical Approaches***

There are a number of techniques, some more mature than others, which can be used to address some of the threats to integrity of election results in the context of remote electronic voting. A summary of these techniques is presented below.



### 5.4.1 Cryptographic Integrity Protection

The data which travels through the Internet between the voting system and the voter's computer can be efficiently protected from en-route modifications via protocols like Secure Socket Layer (SSL) and Transport Layer Security (TLS). SSL and TLS are widely used to protect the integrity of communications between web servers and browsers and are frequently used in other applications as well such as email client and server communications. When used with mutual authentication, these protocols provide end-to-end security. In addition, cryptographic integrity protections, such as digital signatures and message authentication codes, can detect any changes in data as it is transmitted from one system to another. Cryptography can be very effective at protecting data in-transit and at-rest. However, cryptographic integrity protections do little to protect data as it is being processed on voting system components, such as when cast votes are constructed on client machines, or when they are tabulated on back-end equipment.

### 5.4.2 Advanced Cryptographic Voting Techniques

A specific research area in cryptography has been investigating more secure voting protocols to protect ballot secrecy, while at the same time offering unique integrity protections. These protocols, often called end-to-end cryptographic voting protocols, may be able to detect certain types of attacks where the election outcome is not the result of the aggregation of all cast votes. They can produce irrefutable proofs of tampering, even if a small number of cast ballots have been modified or deleted. Both voters and the general public can check that all cast ballots have been correctly tallied by the voting system. Additionally, end-to-end cryptographic voting protocols may allow each voter to verify that his/her vote appears in the final tally. There is a high degree of overlap between these protocols and the cryptographic protocols previously described in Section 4.4.2 to protect ballot secrecy.

The threat model for end-to-end cryptographic voting systems often assumes attackers have compromised the back-end voting system software. Thus, these systems can provide protection against attacks when cast ballots are modified in-transit or stored on voting system back-end equipment, and attacks that modify ballots or cause them to be incorrectly tabulated.

However, there are many types of attacks on voting systems that are not mitigated by end-to-end cryptographic voting protocols alone. In general, end-to-end cryptographic voting protocols may do little to mitigate client-side security threats, as cast ballots can be modified as they are constructed on the client machine. While end-to-end cryptographic voting protocols allow

the voter, or their proxy, to detect changes to cast ballots after they are constructed on a machine, they provide limited or difficult means to check the constructed cast ballot actually corresponds to the voter's choices. However, systems that provide clear text receipts of voters' choices are much easier to check, but these systems present potential problems with ballot secrecy and coercion. In addition, end-to-end cryptographic voting protocols do little to protect against attacks where voters' authentication credentials are stolen or sold.

At this time, there have been no formal usability or accessibility studies of current cryptographic voting schemes, but researchers anticipate that such studies would identify issues that would need to be addressed.

Remote electronic voting systems using end-to-end cryptographic voting protocols have been fielded in a limited number of pilots, including a university election at the Université Catholique de Louvain in March of 2009 [23]. End-to-end cryptographic voting protocols are an ongoing area of research, and researchers in academia and industry are coming up with different methods to address the shortcomings of these techniques.

#### **5.4.3 Use of a Voter-Held Trusted Hardware Component**

The threat posed by client-side vulnerabilities might be significantly reduced if the voter could use a third computing device that could communicate with the client machine and which could reasonably be assumed to be secure. Smart-cards and cell phones could, in principle, play this role. But it may be too expensive to add this capability to these devices for the sole purpose of voting, but this could be implemented to also help secure electronic commerce transactions.

#### **5.4.4 Malware Detection/Prevention Software**

Many commercial and free tools protect against malware, including antivirus and anti-spyware programs. These tools typically work by scanning files downloaded or opened on a computer. The tools look for patterns in files that match those of known malware. This is called signature-based detection. Many newer forms of anti-malware software can do more sophisticated heuristic-based checking in addition to signature detection to identify new malware. However, this is generally only effective at identifying new variants of an already-known piece of malware.

Anti-malware programs do not completely mitigate the threat of malware. Because anti-malware programs are dependent on an up-to-date list of malware signatures, users must update their anti-malware programs

frequently. In addition, anti-malware programs are not effective against new types of malware that have not yet been identified by vendors of anti-malware software and added to signature lists. Even known malware can be difficult to detect, as there are several techniques for writing malware to try to avoid signature-based detection. Once a computer is infected with malware, antivirus software may fail to detect or remove the virus. Some malware disables anti-malware software running on infected machines in ways that are not easy to detect.

#### **5.4.5 Remote Software Verification**

One area of research and development is remotely verifying that a piece of software on a given computer has not been tampered with. The most common application for this technology is to limit cheating in online gaming. In some online games, hackers have discovered ways of modifying software on their system to give them an unfair advantage. These anti-cheating mechanisms check the integrity of gaming software and data files looking for known cheating software in memory. It may be possible to extend these ideas to remotely inspect a voter's computer for malware.

Some current virtual private network software distributions include mechanisms to do end-point security scanning. When connecting to a server, the client machine downloads software from within the browser (often a Java application or ActiveX control) which performs some security scans on the client machine and relays the results to the server. Typically the purpose of scanning the system is to enforce an organization's security policy, such as running up-to-date antivirus software and a properly patched operating system.

An area of active research and development that may bring about more rigorous methods for remote software attestation is trusted computing platforms. In the future, it may be possible to use trusted computing modules (TPM) in voters' computers to demonstrate to an Internet voting system server the computers are in a desired state free of malware capable of tampering votes. The use of TPMs in voting systems is an active research area, with researchers proposing different methods for their use in voting systems [22][24]. While much of this research is focused on using TPMs in Direct Record Electronic (DRE) systems, the ideas could be extended for use in personal computers and Internet voting system servers. However, there are significant technical challenges to finding a workable solution. Furthermore, if and when solutions are found and implemented, deployment of the necessary hardware and software would likely be slow.

#### **5.4.6 Formal Verification of Software**

Formal verification of software involves providing mathematical proofs of the correctness of a given piece of software. In order to do formal verification, it must be possible to very precisely describe correct behavior in an algorithm. For this reason, formal verification is very hard to do for large software systems since it is difficult to precisely capture the behavior of a complex system. However formal verification is sometimes done for smaller pieces of a larger software system, such as the software implementing a cryptographic algorithm or protocol. Formal verification of software is very expensive, and is only done in extraordinary applications. For example, the INTEGRITY-178B real-time operating system, one of only two formally-verified operating systems, is used in military and commercial avionics.

Formal verification of system designs, while still uncommon, is required at Evaluation Assurance Levels 5, 6 and 7 of a Common Criteria security evaluation [25]. Again, these often involve verifying only a small piece of software within a larger system.

Because of its considerable cost, formal verification of software or designs is likely not well-suited to mitigating risks of software defects or vulnerabilities in remote electronic voting systems.

#### **5.4.7 Preconfigured Bootable Environments**

One method proposed for dealing with client-side security issues on voters' personal computers is to give voters a known-secure voting environment. This could be accomplished by distributed bootable media, such as CDs, DVDs, or USB drives that have been preconfigured with security hardening, and for connecting only to the Internet voting servers.

However, this approach has several significant disadvantages. One of the arguments for remote electronic voting has been the difficulty of distributing election materials to voters. Bootable media would likely have to be distributed by mail and would pose similar delivery challenges, such as obtaining up-to-date mailing address information for each voter. In addition, it would be very difficult to guarantee the bootable media would work on the vast majority of voters' personal computers. And, perhaps most significantly, it may be very hard for voters to identify legitimate bootable media from fraudulent media. Rather than serving to protect voters from malicious software, this could provide an avenue for attackers to distribute their own bootable media with malicious software preinstalled.

#### **5.4.8 Virtualization Technologies**

A possible way of bypassing some of the logistical problems of creating and distributing bootable media may be to use virtualization technology to run a clean voting environment in a virtual machine. That is, software running on a voter's computer could simulate a computer free of malware. This could alleviate some of the problems associated with bootable media including appropriate drivers and ensuring the default configuration would be compatible with a given user's network. Nonetheless, there are still significant logistical problems associated with attempting to securely distribute virtual machine images to voters. And, as was the case with bootable media, there remains the potential problem of voters using virtual machines pre-loaded with malicious software.

Generally, virtualization technology has been concerned with protecting the host operating system that is running the virtual machine software from any malicious or unreliable software running on the virtual machine's operating system. However, vendors of virtualization technology are beginning to implement systems that provide some protection against unauthorized modification of virtual machines by applications running on the host operating system. This is an important feature, as the reason for using these virtual machines is to protect voters from any malicious software running on their computers.

#### **5.4.9 Secondary Communication Channels**

While many of the technical approaches described above attempt to deal with the problem of malicious software on voters' computers by either detecting the malicious software or preventing its installation, another approach is to try to make voting from an infected computer reasonably safe. There are methods that attempt to do this using a secondary communication channel between the voter and the election authority that is independent from the voter's channel to the election authority such as the Internet through his or her personal computer. This second channel could be used when voters mark ballots to prevent malicious code from modifying votes in a directed way, or it could be used to confirm voters' selections.

In the first case, voters could be given individualized code sheets with unique random codes assigned to each candidate or choice on the ballot. In this case, the second channel might be the postal mail. To vote for a particular candidate, the voter would have to enter the random code assigned to that candidate on the Internet voting website. Malicious code running on the voter's computer would not know the association between the candidates and random codes, and thus would not be able to change votes to a particular candidate. However, malicious software could still

prevent voters from casting ballots, or try to deceive the voter into giving it the necessary information to change votes. In addition, there are significant usability concerns about this type of approach, in addition to logistical concerns involving the distribution of these code sheets to voters.

Alternatively, the second communication channel could be used to confirm a voter's selections. For example, a voter could be sent a message indicating how he or she voted. In this case, it is important that the second channel offer very fast delivery of messages, like a text message or telephone call, so the voter can confirm their selections in real-time. However, this approach creates some concerns related to vote selling by providing a channel which could be used by a vote buyer to verify how someone voted.

Electronic mail may be a tempting choice for a secondary communications channel, but there are significant drawbacks to using e-mail in this manner. E-mail is not an independent second channel, as the same computer and Internet connection used to construct and transmit the vote would likely be used to receive the e-mail. Malicious software running on the voter's computer may be able to change incoming e-mails along with cast votes.

#### **5.4.10 Messages Computers Can't Understand**

An alternative to using secondary communication channels is to communicate with the voter through the standard channel but coding information in ways that a computer cannot understand such as CAPTCHAs. CAPTCHAs are little puzzles that users are asked to solve, often involving reading distorted text, to prove that a human is accessing a Web application. CAPTCHAs are often used to try to block attacks where automated computer programs access a website and attempt to submit or collect information.

In principle, the whole ballot could be rendered using CAPTCHAs with the voter exercising choices by clicking on the rendered image. In this case, the client-side machine is unable to associate voter choices with locations of clicks. Even without the use of CAPTCHAs, using pointers to images instead of text should make it harder for malware to decode voter choices in order to alter them in favor of a given choice, because this is not a feature offered by currently available malware kits. Further research on these ideas is needed to identify usability and other issues that may arise. Note, these techniques do not stop the client machine from preventing the vote or randomizing it, and introduce usability and accessibility challenges that may not be adequately addressed.

## ***5.5 Open Issues***

Ensuring the security of personally-owned computers remains a very serious open issue. At this time, there is relatively little jurisdictions can do to ensure that voters' computers are free from malware capable of changing ballots cast from those machines. Attackers have demonstrated an ability to infect large numbers of machines with malicious software. Although in the case of UOCAVA voting, attackers would need to successfully target the relatively small percentage of individuals' in the world that are eligible to vote as overseas or military voters. While remote software verification, trusted computing modules, and computer virtualization are potentially promising technologies for mitigating the threat of malware on voters' computers, none of these technologies appear ready for immediate use with remote electronic voting systems.

There are also open issues related to the security of software on voting system servers. While extensive testing may be able to uncover many software bugs, there are no guarantees it can uncover all bugs in the software.

Advanced cryptographic voting technique, specifically end-to-end cryptographic voting protocols, can be highly effective at detecting certain types of attacks on election integrity, including modification or deletion of cast ballots. However at this time, they are most effective against mitigating attacks that take place on the voting system servers. Most of these techniques are not effective at detecting attacks taking place on the computers used to cast ballots. While extending end-to-end cryptographic voting protocols to detect client-side attacks is an active research area, methods that have been proposed are either difficult to use or impractical. In some cases, end-to-end cryptographic voting techniques only detect if an integrity violation has occurred. It may not be possible to recover from the detected error or to measure the extent to which the detected error affects the outcome of the election. Also, end-to-end cryptographic voting techniques may not be able to distinguish between a bug and an active attack. While this is an area of ongoing research and activities, end-to-end cryptographic voting techniques for Internet voting are largely still an academic effort.

## 6 Availability

Availability is used to describe the proportion of time a system is functioning and operating, including times when the system is performing at reduced capacity. Due to resource overload, malicious attack, and system malfunction, a system may become unable to function, and thus is considered unavailable.

### 6.1 Potential Benefits

Electronic transmission of election materials can provide several benefits to UOCAVA voters and election officials compared to alternative voting methods for overseas and military voters. The following section describes some of the potential benefits.

#### 6.1.1 Timeliness of Delivery

Internet voting systems do not suffer from the same delays associated with voting through the postal mail. Postal mail delivery to remote locations can take significantly more time than delivery times within the United States. For example, delivery through the military postal system to Middle East postal offices typically takes 7-12 days [27]. Internet transmission, however, is nearly instantaneous, as long as voting system endpoints (the server and the client) and communication lines are operational.

#### 6.1.2 Receipt Confirmation

The United States Postal Service (USPS) is a relatively reliable delivery mechanism, with first class mail on-time performance exceeding 90% [28]. However, mail to UOCAVA voters must go through other postal services in addition to the USPS, such as the military postal system, or those of foreign nations. Delivery confirmation is an option for USPS mail to military addresses, but is often not an option for mail to and from foreign addresses. Therefore, it is nearly impossible to detect which blank or completed ballots have been lost or delayed in the mail system.

Remote voting over the Internet can provide immediate feedback to senders if there is a transmission problem via real-time confirmation and error messages. This information could be used to detect problems and remediate them.

#### 6.1.3 Flexibility of Physical Locations

Overseas voters, particularly military voters, are a highly mobile population, and are not always quick to inform their local election officials of their new addresses. Remote voting over the Internet allows voters to receive or cast ballots regardless of their physical location.



## **6.2 Properties**

### **Property: Up-time**

*Voters, election officials, and other system operators are able to use the voting system normally for a substantial percentage of the total time allowed to configure the system, cast votes, and tally votes.*

#### **Notes:**

Up-time is a measure of the extent a system is available for use by system operators and users. A number of factors affect up-time, including how often failures occur (see the "Reliability" property) and time it takes system administrators to restore functionality after a failure occurs. System availability can be maliciously targeted by an attacker to disrupt voters from casting their ballots.

### **Property: Reliability**

*The voting system, to a high degree of probability, will remain operational during the election under predefined normal operating conditions.*

#### **Notes:**

Reliability is a measure of the likelihood a system will continue to perform as intended for a specified time under a particular set of predefined conditions. In this case, reliability is referred to as the likelihood the voting system can complete an election without a loss of functionality when it is not facing a malicious attacker.

### **Property: Recoverability**

*Voting system operators are able to restore the system to normal operation in a timely manner when failures occur.*

#### **Notes:**

Voting systems should be designed to limit downtime in the event of failures. In practice this implies a very low probability of catastrophic failure such as loss of stored cast ballots.

### **Property: Fault-Tolerance**

*The voting system is able to continue operation, perhaps at a reduced level of functionality, when failures or attacks occur.*

#### **Notes:**

A common method for achieving some level of fault-tolerance is to use redundant system components or resources.

**Property: Fail-Safe**

*In the event of a failure or attack, the voting system experiences minimal data loss or further damage to voting system components not directly affected by the failure or attack.*

**Notes:**

Fail-safe is a system property which states that voting system failures or attacks should have limited impact on the integrity and availability of system components and data. For example, hardware component failures in the voting system should not result in the loss of cast vote records or audit information. An attack on one component in a voting system should not damage a second component. For instance, an attack on the voter registration database should not harm the voting system web server, although it may inhibit voting activities until the issue with the voter registration database is resolved.

**Property: Scalability**

*The capacity of the voting system can be increased with additional resources (e.g., servers, network bandwidth, etc.) without redesigning the system's architecture.*

**Notes:**

A scalable voting system can grow to accept greater and greater number of voters by adding additional hardware, more powerful hardware, faster network connections, other computing resources, or any combination thereof.

**6.3 Threats to Availability**

Like any information technology system, Internet voting may be the target of denial of service attacks (see [29] for precinct voting denial of service attacks). The potential scale and impact of the attack may be much larger for Internet voting systems than for polling place voting or mail-in voting. The attacks can be targeted towards the server providing the voting service, the personal computers of the voters, or the infrastructure connecting the two. Denial of service attacks may be selective, such as disrupting service for voters deemed likely to cast a ballot in a particular way (e.g., a particular demographic group).

**6.3.1 Large-Scale Denial of Service**

Denial of service attacks are a type of attack where malicious individuals attempt to make a computer system unavailable to its users. Depending on

the nature of the attack, and on its target, a denial of service attack can be anything from a minor nuisance to a devastating attack.

Denial of service attacks could prevent voters from being able to cast votes either by making Internet voting system servers inaccessible or disrupting systems they rely on, such as the communications infrastructure or voter registration database. Aimed at the back-end of the voting system, these attacks could prevent large numbers of people from casting ballots over the duration (anywhere from hours to days) of the attack.

Denial of service attacks of varying severity occur frequently on the Internet. The type of target and motivation differs from attack to attack. A frequent motive of attackers is political in nature, with attacks carried out by individuals or groups disagreeing with the victim's views. Large corporations, nation states, and the communications infrastructure are frequent targets for attack. For example, in 2007 the nation of Estonia was targeted with a large-scale denial of service attack [30], with the nation of Georgia experiencing a similar attack in 2008 [31]. Critical portions of the Domain Name System (DNS) have also been targeted with attacks, including distributed denial of service attacks against root DNS servers in 2002 [32] and 2007 [33].

Denial of service attacks can be conducted in a variety of ways, but most major attacks are distributed denial of service attacks. Collections of malware infected computers, known as botnets, can be purchased or rented by attackers to be used to attack a target organization.

### **6.3.2 Selective Disruption and Suppression**

While denial of service attacks can cause voter disenfranchisement on a significant scale, their ability to impact the outcome of an election is somewhat limited unless the attack is focused on a particular demographic or jurisdiction. However, targeted denial of service attacks have been documented. In 2009, denial of service attacks targeted a specific Georgian blogger on Twitter, Facebook, Livejournal and Google [34]. Denial of service attacks that selectively disrupt systems at a particular jurisdiction or certain voter demographic could not only result in voter disenfranchisement, but also sway the results of an election.

Remote electronic voting may make it harder to prevent a voter from attempting to vote when the voting system is architected to function and operate even under vote suppression attacks. On the other hand, some cyber attacks, such as denial of service attacks, may make it easier to thwart an attempt to vote due to the resources available to an attacker in the form of computers controlled by botnets.

### **6.3.3 Client-Side Disruption**

While most large-scale attacks on availability target one of the voting system's servers or the communications infrastructure, attacks can also target the voters' machines. Malware on voters' computers could prevent them from accessing voting web sites.

## ***6.4 Current and Emerging Technical Approaches***

While there is no general solution to denial of service attacks, a series of techniques can be used to prevent, detect and speed up recovery from such attacks.

### **6.4.1 Redundancy and Over-provisioning**

The most widely used approaches for achieving high-availability systems include the use of redundant systems and over-provisioning of system resources. At a basic level, these approaches involve fielding systems with excess capacity so they are able to better handle failures on certain system components or attacks.

Redundancy involves the duplication of critical system components. The duplicate components are used as backups in the event of failures or to augment capacity in the event of a spike in legitimate or illegitimate traffic. For instance, a system could be designed with redundant web servers such that the backup system can take over the expected load in the event the primary system fails.

A more general approach, called over-provisioning of system resources, involves fielding systems capable of handling a much greater load than would be expected under normal conditions. A useful strategy is to identify possible performance bottlenecks in the system and to augment the capacity at those bottlenecks. Possible bottlenecks include capacity and performance of the communications lines, support infrastructure (such as firewalls and routers), or database and web servers. Over-provisioning can involve any combination of duplicating resources (e.g., mirrored sites located at multiple physical locations) or making individual resources more powerful or abundant (e.g., faster network connections, more powerful servers, etc.) than would ordinarily be needed.

Fielding over-provisioned systems can be costly, particularly for relatively small systems such as Internet voting systems that are rarely used and have less traffic than major e-commerce web sites. Small increases in system capacity are not likely to deter or prevent attacks on availability, but large

increases in capacity may be wasteful and still potentially ineffective. Over-provisioning raises the bar for attacks but does not make attacks impossible.

#### **6.4.2 Detecting Active Attacks on Availability**

Compared to other types of attacks on voting system, availability attacks are usually relatively easy to detect by system administrators. In some cases, the system crashes or becomes unavailable to all users. At this point, voters have already been affected and will continue to be affected until the attack is successfully repelled. The key to maximizing availability in the face of denial of service attacks is early detection and quick reaction.

#### **6.4.3 Defending Against Active Attacks**

The most common approach for defending against denial of service attacks is over-provisioning, which provides protection against all kinds of incidental or malicious threats to availability. However, there are a number of other things system designers and administrators can do to defend against attacks.

One approach is to preemptively harden systems against denial of service attacks. Hardening voting systems include identifying and fixing bottlenecks as well as vulnerabilities in host systems that make denial of service attacks easier to carry out, and carefully designing the internal network infrastructure. In some cases, there may be multiple technical options for designing a secure and usable voting system that works equally well for their intended tasks but may be more resistant to denial of service attacks.

Another approach is to filter dangerous network traffic containing known attacks carefully constructed to crash or overwhelm a particular system resource. Once an active denial of service attack is detected, an organization may be able to filter out the network traffic making up the attack. While network traffic filtering can be done on the border of an organization's network, an attack may attempt to overwhelm the filtering mechanism or merely fill the in-bound network connection. In these cases, it is helpful to filter attack traffic closer to the source, which usually requires the help of third-party Internet service providers.

Some distributed denial of service attacks work on the premise an attacking client can force a server or other device to consume far more resources than those required by the client to conduct the attack. For example, establishing a Transmission Control Protocol (TCP) connection with the server requires that the server allocate resources before the client. There are approaches that attempt to address the client server resource imbalance, such as SYN

Cookies and proof-of-work techniques, by forcing clients to allocate some resources before establishing a connection with a server [35].

#### **6.4.4 Cloud Computing**

In protecting system availability, there is strength in numbers. Having redundant systems to migrate to after a failure, or having excess capacity to raise the bar for denial of service attacks, can help systems achieve higher levels of availability. However, purchasing, deploying and maintaining this excess capacity may be cost-prohibitive. An emerging area in the computer industry is a concept known as cloud computing. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [36].

In the cloud computing model, a large pool of resources can be distributed between many different applications and even customers. Excess capacity in the system can be applied to any of the applications running in the cloud on an as-needed basis, and the cost associated with maintaining the excess capacity can essentially be distributed across all of the customers. In the event of a hardware failure on a particular machine in the cloud, any applications running on that machine can be almost immediately transferred to a different physical machine in the cloud. In the event of a spike in traffic for a particular application, additional physical or logical machines, network bandwidth, or other resources could be allocated to that application.

However, in cloud environments, multiple applications are being hosted on the same systems. So, in the case of an Internet voting system, the voting system may be running on the same equipment used to perform completely unrelated tasks. When a service provider manages the cloud, each customer may have little control of what other applications coexist on the same physical equipment. Typically, virtualization technology is used to keep different application resources logically, rather than physically, separate. However, this introduces new security issues researchers have only begun to look at in the last few years.

Cloud computing appears to be a very promising technology for increasing system availability in a cost-effective manner, but it is not clear if it is ready or suitable for use with remote electronic voting systems.

## ***6.5 Open Issues***

Most defensive techniques against denial of service attacks can raise the bar for an attacker to successfully mount an attack but cannot guarantee protection. In fact, due to the nature of the Internet, it may not be possible to provide complete protection from certain types of availability attacks. Given the commercial availability of botnets for use in distributed denial of service attacks, attacks on availability are a very real threat to Internet voting systems.

However, Internet voting systems are no more vulnerable to denial of service attacks than many other types of online computer systems as, at a high-level, their architectures have many similarities. And, the threats to voting system availability should be considered relative to availability issues faced by mail-in absentee voting, including undeliverable mail due to a frequently moving overseas voting population and the time necessary to send or return election materials.

Cloud computing appears to be a promising technology. However, it is a young field where researchers and developers in industry and academia are making advances at a rapid pace. The security issues associated with cloud computing, along with new types of potential vulnerabilities, continue to be identified.

## 7 Identification and Authentication

Determining if a user is authorized to use a voting system includes the distinct steps of identification and authentication. Identification is the act or process in which an entity (e.g., user or system component) provides a unique identity so a system can distinguish the entity from all others. Authentication is the process of establishing confidence in user identities.

Proper voter authentication is required to ensure only eligible voters can cast ballots and a valid voter contributes a single ballot to the final tally. A remote voting system will typically verify credentials it is provided with, and assume the person providing those credentials is the legitimate owner. As credentials may come from the voter's computer rather than from the human voter him or herself, the voter's computer may gain direct, unrestricted access to the voting credentials. The binding between voters and identities, and between identities and credentials, is established through "voter identification."

It is also important, in a remote setting, that the voting system authenticates itself to the voter. This implies that the voter is able to check that she is actually interacting with the legitimate Internet voting service.

### 7.1 Potential Benefits

Polling place voting typically authenticates voters by having polling place officials interact directly with the human voters. In some cases, voters may be asked for identification or some other authenticator. In Internet voting, strong cryptographic credentials can be used to authenticate voters. In such cases, cryptographic authentication mechanisms make it essentially impossible to trick the system into accepting forged credentials.

#### 7.1.1 Automated Authentication Mechanisms

Hand signature verification generally requires trained election workers to inspect every ballot package returned by voters, matching the signature included with the ballot to a signature specimen on file. While some absentee voting management systems can automate some of the signature comparisons, it is still a moderately resource intensive activity. However, electronic authentication methods can be entirely automated.

#### 7.1.2 Strong Remote Authentication

Currently, remote electronic authentication methods exist which are capable of providing high levels of assurance of a user's claimed identity. Many of these methods are widely deployed in the public and private sectors.



Although the stronger authentication mechanisms are typically used in government, military or corporate environments, they have not been widely deployed to general public. For instance, the federal government's Personal Identity Verification program of the federal government involves distributing smart cards to government employees and contractors for authentication purposes. The Department of Defense's Common Access Card is similar program for military personnel and contractors. However, most citizens of the United States that are not associated with the federal government or military so do not have smart cards. The situation in the United State is different from other countries that have deployed Internet voting systems, such as Estonia, which have smart cards deployed to the vast majority of the general population.

## **7.2 Properties**

### **Property: Voter Identification**

*Election authorities and voting systems are able to uniquely identify eligible/registered voters within a particular jurisdiction.*

#### **Notes:**

Unique identification of voters is necessary to bind eligible voters to digital identities and digital identities with credentials. The credentials are used for voter authentication and enforcing access control rules and keeping records of who did what on the voting system.

### **Property: Voter Authentication**

*The voting system verifies the credentials of potential voters before allowing them to perform any authorized actions on the system.*

#### **Notes:**

The voting system should ensure that voters connecting to the system are eligible to use the system to perform the requested functions (e.g., cast a ballot, update voter registration information). In remote authentication, it is important to understand there is no difference between authentication of voters and authentication of credentials. That is, anybody with access to the voter's credentials is able to impersonate the voter. There is a spectrum of techniques that offer different levels of assurance in remote authentication. For example, 4-digit pins offer lower remote authentication assurance than strong passwords. Higher assurance can be obtained using "two-factor authentication" methods typically involving cryptographic token and a PIN, a password and a biometric, or a time-dependent random number generated by a small hardware device issued to the user. Voting system authentication in the foreseeable future is unlikely to make use

of biometrics, but deployment of some form of two-factor authentication does seem feasible for special populations such as military personnel. For instance, the Department of Defense has distributed the smart card-based Common Access Card (CAC) [43] to nearly all of its military personnel, employees and contractors.

Voter authentication should not compromise the secrecy of the vote. The authentication protocols should not attach easily retrievable or inferable voter identification information to cast ballots. If jurisdictions allow a voting system to attach voter identification information to cast ballots, then this information should be encrypted in such a way that it can only be decrypted under exceptional circumstances.

### **Property: Administrators/Officials Identification**

*Election authorities, system administrators, or other individuals with administrative access to voting systems, are uniquely identified by the voting system.*

#### **Notes:**

Individuals with privileged access to the voting system should be uniquely identified by the voting system. That is, system administrators, election officials, and other with access to voting system should not share accounts or login credentials. This allows for greater accountability of administrative actions performed on the voting system.

### **Property: Administrators/Officials Authentication**

*The voting system components verify the credentials of system administrators, election officials, and other election insiders before allowing them to perform any actions, as authorized, on the system components.*

#### **Notes:**

Voting system administrators and election officials do not require the same privacy protections as voters. Thus, every voting system component should verify the unique identity of the official or administrator before granting them access to the system.

### **Property: System Component Identification**

*Each voting system component is identified by the system.*

#### **Notes:**

Like users, each voting system component should be identified. While some level of unique identification would be necessarily for various

administrative functions for logistical reasons, groups of components that act as one might be identified as part of a collective group. For instance, individual machines in a group of web servers behind a load balancer may all share the same identity for identification and authentication purposes.

### **Property: System Component Authentication**

*Users and system components should verify the identities of voting system components before any other interactions with those components.*

#### **Notes:**

It is important to note that this property applies both to users (e.g., voters, election officials, administrators) connecting to voting system components, as well as voting system components connecting to other components. In both cases, users and voting system components connecting to the voting system should verify they are communicating with the component they intended and not some other computer system impersonating the intended component. In particular, voters should authenticate the voting system they are interacting with, to ensure it is the legitimate voting system.

### **Property: Non-transferable Credentials**

*It should be difficult for voting system credential holder to pass his or her credentials to an unauthorized party without detection.*

#### **Notes:**

Section 7.3 discusses several threats to identification and authentication systems where an attacker convinces a legitimate user to disclose credentials to an unauthorized party. In most cases, this would involve deceiving the legitimate credential holder but could be done with the cooperation of the credential holder (e.g., in the case of vote selling). Credential transfer attacks should be difficult to perform without detection. In this case, difficult may mean the attack does not scale well, or that the threat of punishment if caught is severe enough to deter attacks.

## ***7.3 Threats to Identification and Authentication***

### **7.3.1 Unauthorized Issuance of Credentials**

One common threat to identification and authentication systems is that unauthorized parties may be issued credentials they are not eligible for. For instance, an individual may impersonate some other individual and register

in his or her name. Alternatively, an individual who is not eligible to vote in a jurisdiction may register to vote and be issued credentials to vote. These types of threats are very similar to current forms of voter registration fraud.

There continues to be disagreement over the extent and severity of voter registration fraud in the United States. A study of election crimes by the Election Assistance Commission found that while experts agree fraudulent voter registration forms are filled out, most do not believe these fraudulent registrations result in fraudulent votes actually being cast [37].

It is not known how a move to remote electronic voting over the Internet will change the threat environment for these forms of voter registration fraud.

### **7.3.2 Phishing/Pharming**

Phishing and pharming are two related attacks on the Internet today. While the method for conducting the attack differs between the two, the goal of the attacker is the same: to trick users into revealing their credentials on an illegitimate web site that looks like the legitimate site. In the case of phishing, an attacker sets up a fake website and lures users to the site. Attackers use a variety of means to lure users to these websites, but they typically involve registering a website domain name similar to the legitimate web site and sending mass e-mails claiming to be the legitimate website owner but including links to the fake website. Phishing is largely an attack on the user, rather than on any particular piece of equipment. Pharming is a similar attack, except rather than tricking a user into visiting the fake web site, attackers use some sort of computer or network vulnerability to redirect a user from the legitimate website to an illegitimate one without the user's knowledge.

Phishing attacks are very widespread on the Internet, with credentials to financial and social networking sites often being the target of the attacks. According to a Gartner report, five million consumers in the United States lost money to phishing attacks in fiscal year 2008 [38]. Their survey estimated the average consumer loss per successful phishing attack was \$351. However, accurate information on the losses associated with phishing is very difficult to collect, and other researchers have questioned the accuracy of this information, claiming that actual losses are much lower [39]. A recent report by the Anti-Phishing Working Group found phishing attacks continue to be a significant problem, with a record number of organizations targeted by phishing attacks in the fourth quarter of 2009 [40].

Phishing and pharming attacks on Internet voting systems could successfully steal voters' credentials, allowing malicious parties to cast votes in place of the legitimate voters. Attackers may also conduct more targeted phishing attacks, sometimes called spear phishing, on election system administrators or election officials, possibly resulting in gaining privileged access to back-end voting system equipment. Because these attacks are just as much attacks on human users as they are on the technical system, they are very difficult to prevent. Phishing attacks in particular require very little resources and technical expertise to conduct, yet can impact a very large number of people. While Section 7.4.5 will discuss a common method for preventing phishing and pharming attacks, its benefits are somewhat limited.

### **7.3.3 Credential Selling**

Some types of credentials are very easy to transfer to another individual. For instance, PINs and passwords can be physically or electronically sent to another individual as part of a vote selling attack, as described in Section 4.3.3 or in attempts to coerce voters, as described in Section 4.3.2. As noted in those sections, it is difficult to estimate the likelihood of such attacks or how motivated potentials attackers would be to conduct these types of attacks. However, depending on the types of credentials used, these attacks could scale fairly well, potentially allowing individuals or organizations to collect large numbers of voters' credentials and cast votes on their behalf.

There are technical measures that could be taken to greatly limit the ability of these attacks to scale, such as using credentials that cannot be easily passed from a voter to another individual. For instance, use of hardware tokens, such as smart cards or one-time password devices, could require a voter and coercer/vote-buyer to exchange a physical device. However, these mechanisms typically come at a higher cost than simple authentications based on passwords or PINs. Biometric characteristics used in conjunction with challenge-response protocols may also be used to make it impossible to transfer a person's credentials to someone else.

### **7.3.4 Social Engineering**

Social engineering is a class of attack where malicious (or curious) individuals manipulate legitimate users of a system into divulging sensitive information, such as login credentials for a system. Phishing and pharming can be considered a type of large-scale, automated social engineering attack, but social engineering attacks could be highly targeted and interactive. For instance, an attacker conducting a social engineering attack could call an election official or system administrator claiming to be from the service provider hosting the voting system and convince the victim to divulge his or her password.

Social engineering is a class of attacks, and the objective of the attacker may not be solely to steal login credentials. The objectives of social engineers can be to obtain any type of sensitive information that may help them conduct an attack.

### **7.3.5 Cracking/Guessing**

Depending on the type of authentication mechanism used and the location of the attacker, a malicious individual may be able to steal authentication credentials with brute force. This is particularly true for authentication mechanisms like passwords or PINs, as well as knowledge-based authentication. For example, a randomly-generated four-digit PIN has ten thousand different possible values, so an attacker has about a 0.5% chance of guessing a PIN after 5 attempts. In the case of user-chosen passwords, people tend to choose dictionary words for passwords, making it easier for attackers to guess or crack a password.

There are a number of methods that system designers can use that can make it very difficult to guess or crack a particular individual's login credentials. However, if a system has a large number of users, it is much more difficult to ensure that none of the users' credentials are cracked or guessed. This may not be a serious concern for voters' credentials, as these attacks do not appear to scale well.

More seriously, individuals with some level of access to the system, such as physical access to voting system equipment or the ability to watch network traffic between voting system components, may be able to use more sophisticated cracking or guessing attacks. This could be the first stage of an attack if the person is some sort of election system insider (e.g., a computer technician at the service provider hosting the system), or it may be done by a remote attacker that has already gained limited access to the voting system equipment. The impact of these attacks can vary. An attacker that successfully guesses or cracks the credentials associated with a privileged account would be able to perform any actions on the system as if they were the legitimate user.

### **7.3.6 Malicious Software**

Malicious software, or malware, on computers of users' connecting to the voting system could steal credentials used to authenticate to the system. For instance, a common example of malware used by attackers is a keylogger. Keyloggers can record everything that users type on their keyboards. Therefore, it is capable of capturing authentication credentials like

passwords and PINs very easily and can pass them to a remote attacker over an Internet connection. Keylogging functionality is common in malicious code associated with botnets, which were previously discussed in Section 5.3.4.

As was the case with credential guessing and cracking, the impact of these attacks can vary. Attackers that steal the credentials associated with a voter's or administrator's account would be able to perform any actions on the system as if they were the legitimate user. This means that attackers may be able to cast votes in place of a voter, or even perform administrative functions if they are able to get malicious software on a computer used for system or election administration.

### **7.3.7 Insiders/Credential Issuers**

If voting credentials are issued by a particular entity, such as the election officials giving voters usernames and passwords, these insiders have access to all the credentials used for casting ballots. Such an individual may use these credentials to cast votes in the name of voters (for example for voters who did not cast ballots until a couple of minutes before the polls close).

To avoid such scenarios, it may be best to have the voter choosing their own credentials, with insiders never having access to these credentials in clear text, but at the same time being able to check that the voter have knowledge/access to them. For example, if electronic signatures are produced using smartcards, the private keys have to be generated inside the smartcards and it should be impossible to read the clear text private keys, but only to use it to sign messages.

## ***7.4 Current and Emerging Technical Approaches***

### **7.4.1 Passwords and PINs**

Passwords and PINs remain two of the most common methods for electronic authentication, largely because they are relatively cheap and easy to deploy. Most people use passwords to log into their computers and web-based accounts, including e-mail, social networking sites, and financial sites. Passwords and PINs are typically user-generated, although in some cases organizations or systems will send users pre-generated passwords initially and ask the users to change them when they are first used.

However, passwords and PINs have significant security disadvantages compared to other types of authentication mechanisms. User-generated passwords can often be easily cracked if the attackers have sufficient

information, and they are easily stolen by malware or phishing sites. For these reasons, many organizations are moving away from just using passwords for authentication. For instance, the federal government requires some form of two-factor authentication for remote access to government systems [41], and some financial institutions have begun using two-factor authentication for online banking.

#### **7.4.2 One-time Passwords**

One-time passwords are a common method for deploying two-factor authentication. A one-time password is a password that is only valid for a single transaction and usually a short period of time. In most cases, systems using one-time passwords still use user-generated, memorized passwords, with the one-time password adding an additional layer of authentication.

The difficulty of one-time passwords is organizations need a method for securely distributing these one-time use passwords to their users. This is typically done one of two ways: distributing trusted hardware devices to users or sending them on-demand through a secondary channel such as a cell phone.

Many organizations in the public and private sectors use trusted hardware devices to generate one-time passwords. Organizations must keep track of which users are given what one-time password device. These devices typically continuously generate random codes at regular intervals, such as every 30 seconds. When a user attempts to log into a system, he or she typically must enter both a memorized password in addition to the random code on the one-time password device at that particular moment. The use of a hardware device increases the cost of the system, and the device must be securely distributed to users either in-person, or by some other physical means, and may be lost by users.

Alternatively, one-time passwords can be sent or generated on devices that users already have. For instance, a user may have a piece of software on his or her mobile phone that generates one-time passwords in a similar manner as the hardware device described above. Or an organization may have the mobile phone number for a user and send one-time passwords as text messages on-demand to users attempting to authenticate to the system.

The use of one-time password devices can provide some protection against the threats described in Section 7.3 with some important limitations. Because these passwords are constantly-changing strings, they are very difficult to guess or crack, so malware and phishing sites cannot easily collect large numbers of passwords for later use. However, more



sophisticated attacks can be conducted by malware and phishing sites. If an attacker can capture a one-time password and use it before the user sends it to the legitimate system, the attacker can successfully impersonate that user. This can be accomplished with phishing websites that immediately connect to the legitimate website when a victim enters his or her information, or with malware that passes credentials to an attack in real-time. Both of these types of attacks have been used to attack online banking sites and do not require particularly high-levels of technical expertise. Some malware packages commercially available, as were discussed in Section 5.3.4, include the ability to conduct these types of attacks [42].

### **7.4.3 Cryptographic Authentication**

There are various forms of cryptographic authentication that can be done remotely using cryptographic tokens. These tokens are used in a cryptographic protocol whereby the user proves to the organization authenticating them that he or she has possession of the cryptographic token without having to directly present the token. Authenticating using cryptographic tokens can have very strong security properties and can be implemented such that they are very difficult to crack or steal via phishing.

Cryptographic tokens can be software or hardware based. The difference is whether the cryptographic token is stored on a trusted hardware device, such as a smart card, or whether it is merely a file or piece of software on a computer, mobile phone, tablet PC, or other general-purpose computing device. Software-based cryptographic tokens are vulnerable to theft or tampering but do not require any special hardware. Hardware-based tokens provide greater security.

Hardware based cryptographic tokens often take the form of a smart card. Smart cards are used by many organizations in the public and private sectors for authentication purposes. The Department of Defense has distributed the smart card-based Common Access Card (CAC) [43] to nearly all of its military personnel, employees and contractors. The United States federal government is in the process of implementing a similar program, the Personal Identity Verification card [44], for civilian employees and contractors. In lieu of issuing credentials specifically for voting, UOCAVA voting systems should consider leveraging strong credentials that are already deployed. For example, the country of Estonia, which has a smart card-based national identification card, performed voter authentication in its Internet voting system using the electronic credentials found on the national identification card [45].

Cryptographic authentication is also well-suited for allowing components of the voting system to authenticate to one another. There are a number of networking protocols that allow one component to authenticate to other components. Transport Layer Security (TLS), for example, is a commonly used protocol on the Internet to encrypt traffic between a website and a user's computer and to authenticate the website to the user's system. TLS can also be used to authenticate the client connecting to a server. While client authentication is relatively uncommon in typical e-commerce transactions, it is often used in higher security systems.

#### **7.4.4 Biometrics**

Biometrics are methods for identifying and authenticating individuals based on one or more behavioral or physical traits. Commonly cited biometrics used for authentication purposes include fingerprints, iris recognition, and hand/palm geometry. Biometric authentication can offer high degrees of security depending on the quality of the biometric readers used in the system. However, biometrics are typically used for local authenticating, meaning the user authenticating to a system is in the same physical location as the system. This is because biometrics must be measured by a trusted reader, such as a fingerprint scanner.

Some biometrics are better suited for remote authentication, such as speaker verification. Speaker verification authenticates a user based on their speech patterns. This should not be confused with speech recognition, which recognizes the spoken words, regardless of the identity of the person speaking. Currently, speaker verification methods provide significantly higher error rates than other biometrics [48], but it is an active research area with a number of commercially-available systems. Speaker verification may be suitable as a secondary authentication method or, with improvements to technology, a primary method.

#### **7.4.5 Phishing Filters**

Many modern web browsers and anti-malware software distributions include some type of protection against phishing attacks. These approaches typically involve some combination of whitelisting websites known to be safe, blacklisting websites known to be fraudulent, and, in some cases, using heuristics for all other websites in an attempt to estimate the risk of phishing (e.g., a URL using an IP address instead of a domain name). When a user visits a website that is deemed unsafe, the phishing filter displays either a passive or active warning. An example of a passive warning in a browser is a short warning message, such as "Suspicious Website," placed next to the address bar, but does not require any user input to ignore. An active

warning interrupts the user and requires some sort of input by the user to ignore the warning. For instance, before displaying the phishing website, a browser may display a warning page telling the user the website is a suspected phishing site and asking the user if he or she would like to proceed to the page anyway.

However, the effectiveness of phishing filters is limited by their ability to identify fraudulent websites and how well users heed the warnings. A 2006 study by the Mozilla Project found that between 66% and 82% of fraudulent web sites were detected by the phishing filters used in two popular web browsers [46]. A limited number of usability studies have been done on phishing filters. A 2008 study found that 90% of Internet Explorer 7 users ignored passive warnings from the browser's phishing filter, with that percentage improving to 45% when an active warning was displayed [47]. However, new designs for phishing warnings may be able to improve those rates.

#### **7.4.6 Security Awareness and Training**

Many of the threats described in this section are attacks on users, rather than on the voting system components. In some cases, users are not aware of the security threats faced by a system, or what actions might pose a security risk. Security awareness presentations and materials can educate users about these threats in the hopes that they will be less likely to fall to a phishing or social engineering attack and more likely to use safe computing behaviors. Security training can educate users about relevant security skills and competencies that are necessary for them to conduct their jobs effectively and safely.

Jurisdictions should develop security awareness and training programs for election staff. They may also distribute security awareness materials to voters highlighting recommended security practices and potential threats.

### **7.5 Open issues**

Unlike some the other topics areas described in this document, many of the security challenges associated with identification and authentication of users and voters have commercially-available technical solutions. However, there remain logistical concerns, as well as concerns over the cost of implementing some of these solutions.

Deployment of strong authentication credentials for voters is an issue that would likely be difficult for jurisdictions to manage at this time and could be difficult for the foreseeable future. The authentication methods providing the

## Security Considerations for Remote Electronic UOCAVA Voting

highest levels of assurance of users' identities involve specialized hardware devices that increase the cost of the system and complicate deployment. It may be advantageous for jurisdictions to rely on already deployed authentication credentials, such as the DoD's Common Access Card and the federal government's Personal Identity Verification card, which are already deployed to many overseas voters. However, it is not known if these credentials could be used for voter authentication, or what would be done with the hundreds of thousands, if not millions, of overseas voters that do not have one of these electronic credentials. This could change over time; as more people conduct electronic transactions in their daily lives, it may become increasingly important for all citizens to have strong electronic credentials.

The threat of phishing and social engineering attacks are logistically, and even technically, difficult to mitigate. Cryptographic tokens can provide some protection against phishing attacks, but many other authentication techniques can still fall to variations of phishing and social engineering attacks. Mitigating phishing attacks will likely require a combination of technical controls, possibly in the form of cryptographic tokens, and users better able to understand risks and identify risky behavior.

## 8 Conclusions

This paper identified desirable security properties of remote electronic voting systems, threats of voting over the Internet from personally-owned devices, and current and emerging technologies that may be able to mitigate some of those threats. Based on the capabilities of current computer security and voting technologies, the following three issues remain to be significant challenges faced by remote electronic voting systems.

First, remote electronic absentee voting from personally-owned devices face a variety of potential attacks on voters and voters' personal computers. Since the voter's personal computer is outside the control of election officials, it is extremely difficult to protect against software attacks that could violate ballot secrecy or integrity or steal a voter's authentication credentials. These are serious threats that are already commonplace on the Internet today.

Second, remote electronic voter authentication is a difficult problem. Current technology does offer solutions for highly-secure voter authentication methods, but these may be difficult or expensive to deploy. Personally-owned computers may not be able to interface with these methods, such as having the necessary smart card readers for cryptographic authentication using Common Access Cards or Personal Identity Verification cards.

Third, it is not clear that remote electronic absentee voting systems can offer a comparable level of auditability to polling place systems. Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution.

Many of the current and emerging technologies identified in this report are areas with active research and development. Pilot projects should be encouraged, including those involving the use of voting-specific cryptographic protocols, such as the Helios voting system [23]. Emerging trends and developments in these areas should continue to be studied and monitored.

## References

- [1] Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), (as modified by the National Defense Authorization Act for FY 2005).  
<http://www.fvap.gov/resources/media/uocavalaw.pdf>
- [2] 107th U.S. Congress (October 29, 2002). "Help America Vote Act of 2002 (Pub.L. 107-252)." U.S. Government Printing Office.
- [3] National Institute of Standards and Technology Interagency Report: 7551, *A Threat Analysis on UOCAVA Voting Systems*, December 2008.
- [4] Draft National Institute of Standards and Technology Interagency Report 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2010.
- [5] Draft National Institute of Standards and Technology Interagency Report 7711, *Security Best Practices for the Electronic Transmission of Election Materials*, June 2010.
- [6] U.S. Election Assistance Commission (2010, August 10). UOCAVA Pilot Program Testing Requirements, August 10, 2010. Accessed February 16, 2011 at  
[http://www.eac.gov/testing\\_and\\_certification/eacs\\_work\\_with\\_military\\_and\\_overseas\\_voting.aspx](http://www.eac.gov/testing_and_certification/eacs_work_with_military_and_overseas_voting.aspx)
- [7] EAC (2010, April 26). Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems. Accessed May 10, 2010 at <http://www.eac.gov/program-areas/voting-systems/docs/04-26-10-move-act-report-to-congress-final-congress/>
- [8] M. Volkamer and R. Vogt. Basic set of security requirements for Online Voting Products. Common Criteria Protection Profile BSI-CC-PP-0037, Bundesamt für Sicherheit in der Informationstechnik, Bonn, April 2008.
- [9] Council of Europe. Legal, Operational, and Technical Standards for E-Voting. Recommendation Rec(2004)11, September 2004.
- [10] Federal Voting Assistance Program. *Secure Electronic Registration and Voting Experiment. Threat Risk Assessment- Phase 3*. March 23, 2004.

- [11] McConnell, Steven (2004), *Code Complete (Second Edition)*, Microsoft Press.
- [12] Georgia Tech Information Security Center (2008). *Emerging Cyber Threats Report for 2009*. Accessed May 15, 2010 at <http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf>
- [13] US-CERT (2008, May 16). *Technical Cyber Security Alert TA08-137A: Debian/Ubuntu OpenSSL Random Number Generator Vulnerability*. Accessed May 15, 2010 at <http://www.us-cert.gov/cas/techalerts/TA08-137A.html>
- [14] Symantec (2010, April). *Symantec Global Internet Security Threat Report: Trends for 2009*. Accessed May 15, 2010 at [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_internet\\_security\\_threat\\_report\\_xv\\_04-2010.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf)
- [15] Dierks, T. and Rescorla, E., *The TLS Protocol Version 1.2*, Internet Engineering Task Force, Request for Comment 5246, August 2008, <http://tools.ietf.org/html/rfc5246>
- [16] Atsushi Fujioka, Tatsuaki Okamoto, and Kazui Ohta. A Practical Secret Voting Scheme for Large Scale Elections. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology - AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 244--251, Berlin, 1993. Springer-Verlag.
- [17] Rene Peralta. Issues, non-issues and cryptographic tools for Internet-based voting. In *Secure Electronic Voting* (Boston, 2003), Dimitris A. Gritzalis, editor. Kluwer Academic Publishers, pp. 153-164.
- [18] Lorrie Faith Cranor and Ron K. Cytron, Sensus: A Security-Conscious Electronic Polling System for the Internet. *Proceedings of the Hawai`i International Conference on System Sciences*, January 7-10, 1997, Wailea, Hawaii, USA.
- [19] J. Benaloh and D. Tuinstra. Receipt-Free Secret-Ballot Elections. *Proceedings of the 26th ACM Symposium on Theory of Computing*. Montreal, PQ. May 1994. (New York, USA: ACM 1994), pp. 544—553.
- [20] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. *A secure and optimally efficient multi-authority election scheme*. *European Transactions on Telecommunications*, 8: 481-489, 1997.

## Security Considerations for Remote Electronic UOCAVA Voting

- [21] Premiere Election Solutions (2008, August 19). *Product Advisory Notice*. Accessed May 15, 2010 at <http://www.sos.state.oh.us/sos/upload/news/20081001c.pdf>
- [22] Fink, R.A.; Sherman, A.T.; Carback, R.; , "TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules," *Information Forensics and Security, IEEE Transactions on* , vol.4, no.4, pp.628-637, Dec. 2009.
- [23] Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios, In D. Jefferson, J.L. Hall, T. Moran, editor(s), *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, Usenix, August 2009.
- [24] Nathanael Paul, Andrew S. Tanenbaum, "The Design of a Trustworthy Voting System," Computer Security Applications Conference, Annual, pp. 507-517, 2009 Annual Computer Security Applications Conference, 2009.
- [25] Common Criteria for Information Security Evaluation. Part 3: Security assurance components. Version 3.1, Rev. 3, July 2009.
- [26] Patrick Peterson, Henry Stern. "Botnets Gone Wild! Captured, Observed, Unraveled, Exterminated." Presented at RSA 2010, San Francisco, CA, March 1-5, 2010.
- [27] Testimony of Bob Carey, Director of FVAP. (2010) EAC Public Meeting, Dec. 3 2009. Accessed April 5, 2010 at [http://www.eac.gov/public\\_meeting\\_12032010/](http://www.eac.gov/public_meeting_12032010/)
- [28] United States Postal Service (2007). *2007 Comprehensive Statement*. Accessed March 17, 2010 at [http://www.usps.com/strategicplanning/cs07/chpt5\\_001.htm](http://www.usps.com/strategicplanning/cs07/chpt5_001.htm)
- [29] Alvarez, R. Michael (2005, October 5). "Precinct Voting Denial of Service", *NIST Threats to Voting Systems Workshop*. Accessed March 17, 2010 at [http://vote.nist.gov/threats/papers/precinct\\_dos.pdf](http://vote.nist.gov/threats/papers/precinct_dos.pdf)
- [30] Davis, Joshua (2007, August 21). "Hackers Take Down the Most Wired Country in Europe" *Wired Magazine*. Accessed March 5, 2010 at [http://www.wired.com/politics/security/magazine/15-09/ff\\_estonia](http://www.wired.com/politics/security/magazine/15-09/ff_estonia)



- [31] Markoff, John (2008, August 13). "Before the Gunfire, Cyberattacks" *The New York Times*. Accessed March 5, 2010 at <http://www.nytimes.com/2008/08/13/technology/13cyber.html>
- [32] Vixie, Paul, Sneeringer, Gerry, and Mark Schleifer (2002, November 24). Events of 21-Oct-2002." Accessed March 5, 2010 at <http://d.root-servers.org/october21.txt>
- [33] Internet Corporation for Assigned Names and Numbers. "Factsheet-Root server attack on 6 February 2007." Accessed March 5, 2010 at <http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf>
- [34] Worthham, Jenna, and Andrew E. Kramer (2009, August 7) "Professor Main Target of Assault on Twitter" *The New York Times*. Accessed March 5, 2010 at <http://www.nytimes.com/2009/08/08/technology/internet/08twitter.html>
- [35] D. J. Bernstein and Eric Schenk (1996). *SYN Cookies*. 1996. Accessed May 15, 2010 at <http://cr.yp.to/syncookies.html>
- [36] Mell, Peter and Tim Grance (2009, October 7), *The NIST Definition of Cloud Computing*. Accessed March 2, 2010 at <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>
- [37] U.S. Election Assistance Commission (2006, December). *Election Crimes: An Initial Review and Recommendations for Future Study*. Accessed June 15, 2010 at [http://www.eac.gov/assets/1/workflow\\_staging/Page/57.PDF](http://www.eac.gov/assets/1/workflow_staging/Page/57.PDF)
- [38] Gartner (2009, April 14). *Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008*. Accessed March 5, 2010 at <http://www.gartner.com/it/page.jsp?id=936913>
- [39] Cormac Herley and Dinei Florencio, A Profitless Endeavor: Phishing as Tragedy of the Commons, in *Proc. New Security Paradigms Workshop*, Association for Computing Machinery, Inc., September 2008.
- [40] Anti-Phishing Working Group (2009). *Phishing Activity Trends Report, 4<sup>th</sup> Quarter 2009*. Accessed March 5, 2010 at [http://www.antiphishing.org/reports/apwg\\_report\\_Q4\\_2009.pdf](http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf)

## Security Considerations for Remote Electronic UOCAVA Voting

- [41] Office of Management and Budget (2006, June 23). *OMB Memo M06-16*. Accessed March 5, 2010 at <http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf>
- [42] McAfee Labs (2009). *2010 Threat Predictions*. Accessed April 13, 2010 at [http://www.mcafee.com/us/local\\_content/white\\_papers/7985rpt\\_labs\\_threat\\_predict\\_1209\\_v2.pdf](http://www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threat_predict_1209_v2.pdf)
- [43] Department of Defense. *Common Access Card*. Accessed March 5, 2010 at <http://www.cac.mil/>
- [44] National Institute of Standards and Technology (2009). *About Personal Identity Verification (PIV) of Federal Employees and Contractors*. Accessed March 5, 2010 at <http://csrc.nist.gov/groups/SNS/piv/>
- [45] Estonian National Electoral Committee. *Internet voting in Estonia*. Accessed March 5, 2010 at [http://www.vvk.ee/public/dok/Internet\\_Voting\\_in\\_Estonia.pdf](http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf)
- [46] Mozilla Foundation (2006, November 14). *Firefox 2 Phishing Protection Effectiveness Testing*. Accessed April 5, 2010 at <http://www.mozilla.org/security/phishing-test.html>
- [47] S. Egelman, L. Cranor, and J. Hong. You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings. CHI '08: Proceedings of the SIGCHI conference on Human Factors in Computing Systems. April 2008.
- [48] National Institute of Standards and Technology (2008, August). *The 2008 NIST Speaker Recognition Evaluation Results*. Accessed May 5, 2010 at [http://www.itl.nist.gov/iad/mig/tests/sre/2008/official\\_results/index.html](http://www.itl.nist.gov/iad/mig/tests/sre/2008/official_results/index.html)

**NISTIR 7711**

**Security Best Practices for the  
Electronic Transmission of  
Election Materials for UOCAVA Voters**



[This page intentionally left blank. ]

## NISTIR 7711

# Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters

**Andrew Regenscheid  
Geoff Beier**

*Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930*

September 2011



U.S. Department of Commerce  
*Rebecca M. Blank, Acting Secretary*

National Institute of Standards and Technology  
*Patrick D. Gallagher, Under Secretary for Standards and Technology and Director*

[This page intentionally left blank. ]

## **Abstract**

This document outlines the basic process for the distribution of election material including registration material and blank ballots to Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) voters. It describes the technologies that can be used to support the electronic dissemination of election material along with security techniques – both technical and procedural – that can protect this transfer. The purpose of the document is to inform Election Officials about the current technologies and techniques that can be used to improve the delivery of election material for UOCAVA voters. This document is part of a series of documents that address the UOCAVA voting. The first National Institute of Standards and Technology (NIST) publication on UOCAVA voting, entitled NISTIR 7551 *A Threat Analysis on UOCAVA Voting Systems*, was released in December 2008. In addition to NISTIR 7551, NIST has released NISTIR 7770 *Security Considerations for Remote Electronic UOCAVA Voting, Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting*, and NISTIR 7682 *Information Systems Security Best Practices for UOCAVA-Supporting Systems*.

## Acknowledgements

The authors of this document, Andrew Regenscheid of NIST and Geoff Beier of CygnaCom, wish to thank the state and local election officials who provided us with UOCAVA election procedures in preparation for this document. In particular, comments from Paul Miller, Matt Masterson and Carol Paquette were instrumental in the development of this document. The authors would also like to thank Russell Kasselmann, Helen Purcell, Paul Lux, and the Florida Division of Elections staff. In addition, the authors wish to thank their colleagues who reviewed earlier drafts of this document, particularly Nelson Hastings, Barbara Guttman, Theresa O'Connell, and Quynh Dang.

This document has been prepared by the National Institute of Standards and Technology (NIST) and describes research in support military and overseas voting for the Election Assistance Commission and the Technical Guidelines Development Committee. It does not represent a consensus view or recommendation from NIST, nor does it represent any policy positions of NIST.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by organizations even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, organizations may wish to closely follow the development of these new publications by NIST.



## Table of Contents

<b>1 INTRODUCTION .....</b>	<b>5</b>
1.1 Background .....	5
1.2 Purpose and Scope .....	5
1.3 Audience .....	6
1.4 Organization .....	7
<b>2 OVERVIEW.....</b>	<b>8</b>
2.1 Types of Election Materials.....	8
2.1.1 Dissemination of Election Information Materials.....	8
2.1.2 Distribution and Receipt of Voter Registration/Ballot Request Forms 8	
2.1.3 Blank Ballot Delivery .....	9
2.2 Electronic Delivery Options .....	10
2.2.1 Fax .....	10
2.2.2 Electronic Mail .....	11
2.2.3 Web-Sites .....	15
2.3 Cryptography .....	17
2.3.1 Cryptographic Confidentiality Protections.....	17
2.3.2 Cryptographic Integrity Protections.....	18
2.3.3 Cryptographic Protocols .....	19
2.3.4 Digital Certificates.....	19
2.3.5 Certificate Authorities .....	20
<b>3 TRANSMISSION OF REGISTRATION/BALLOT REQUEST MATERIALS.....</b>	<b>22</b>
3.1 Overview.....	22
3.2 General Issues .....	22
3.2.1 Voter Registration .....	22
3.2.2 Voter Authentication.....	23
3.2.3 Protecting Personal Voter Information .....	24
3.2.4 Preparing Registration/Ballot Request Forms.....	25
3.3 Fax.....	26
3.4 Electronic Mail.....	27
3.4.1 Delivery .....	27
3.4.2 Reception of Forms.....	28
3.5 Web-based Distribution and Reception of Forms.....	29
3.5.1 Delivery .....	29
3.5.2 Reception.....	29
3.6 Online Voter Registration Systems .....	31
<b>4 DELIVERY OF BLANK BALLOTS.....</b>	<b>33</b>
4.1 Overview.....	33

4.2	General Issues .....	33
4.2.1	Voter Identification and Authentication.....	33
4.2.2	Ballot Accounting .....	34
4.2.3	Return Identification .....	35
4.2.4	Ballot Tracking.....	35
4.2.5	Ballot Preparation.....	36
4.3	Fax Transmission.....	37
4.4	Electronic Mail.....	38
4.5	Web-Based File Repositories.....	39
4.6	Online Ballot Markers .....	39
<b>5</b>	<b>OTHER RESOURCES.....</b>	<b>42</b>
<b>6</b>	<b>REFERENCES.....</b>	<b>44</b>
<b>APPENDIX A:</b>	<b>GENERAL COMPUTER SECURITY BEST PRACTICES....</b>	<b>47</b>
A.1	System Characterization.....	47
A.2	Identification of Common Controls .....	49
A.3	Network and Communications Protections.....	51
A.4	Configuration Management .....	51
A.5	Contingency Planning.....	53
A.6	Incident Response .....	54
A.7	Continuous Monitoring.....	55
<b>APPENDIX B:</b>	<b>COMPONENT SECURITY CONSIDERATIONS .....</b>	<b>57</b>
B.1	Network Infrastructure Protections.....	58
B.2	E-mail Server Security .....	60
B.3	E-mail Client Security.....	62
B.4	Web Server Security .....	63
<b>APPENDIX C:</b>	<b>GLOSSARY.....</b>	<b>67</b>

## 1 Introduction

To support State and local election officials in carrying out their responsibilities under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), the Election Assistance Commission (EAC) requested that the National Institute of Standards and Technology (NIST) develop security best practices to assist jurisdictions wishing to use electronic means to send or receive voter registration materials and ballot requests, or to distribute blank ballots to overseas and military voters. Many jurisdictions across the country already use electronic mail and fax for these purposes, and some jurisdictions have begun to use Web sites to distribute or collect this information.

### 1.1 Background

In December 2008, NIST released NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems* [1], which documents the threats to UOCAVA voting systems using electronic technologies for all aspects of the overseas voting process. NISTIR 7551 identifies a number of threats to using electronic technologies to obtain voter registration materials, deliver blank ballots, or return cast ballots, emphasizing the need for implementing strong and comprehensive security controls to mitigate the identified threats. That report concluded that existing widely deployed technology can be used to safely expedite the transmission of voter registration and ballot request materials, as well as blank ballots.

### 1.2 Purpose and Scope

This document first outlines the basic process for the distribution of election material including registration material and blank ballots to UOCAVA voters. It then describes the technologies that can be used to support the electronic dissemination of election material along with security techniques – both technical and procedural – that can protect this transfer. The purpose of the document is to inform Election Officials about the current technologies and techniques that can be used to improve the delivery of election material for UOCAVA voters.

This document provides security best practices for the delivery and receipt of documents such as voter registration applications and absentee ballot request forms, and the distribution of blank ballots to overseas and military voters using electronic mail or Web sites. It does not address remote electronic voting systems or the electronic return of cast ballots.

This document is part of a series of documents that address UOCAVA voting. In addition to NISTIR 7551, NIST has released NISTIR 7682 *Information Systems Security Best Practices for UOCAVA-Supporting Systems* [2]. NISTIR 7682 is a companion document to this document, NISTIR 7711. While this document covers security best practices and considerations for electronic transmission of UOCAVA election materials for election officials, NISTIR 7682 provides general computer security best practices for IT professionals charged with configuring and administering IT systems used to support UOCAVA voting. Jurisdictions should consult NISTIR 7682, and other NIST computer security guidelines, for general computer security best practices prior to deploying and using an IT system to support voter registration, ballot request, and blank ballot delivery activities. The best practices in this document are intended to extend, not override, the best practices in NISTIR 7682.

In addition to these security-focused documents, NIST released a document highlighting important human factors issues in UOCAVA voting systems, *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting*, in 2011 [23].

Jurisdictions seeking best practices related to election management, including election management for UOCAVA voting, should consult the EAC's *Election Management Best Practices* document [28], as well as their existing best practices for facilitating UOCAVA voting [29].

### **1.3 Audience**

The intended audience for this document is election officials who are considering the use of electronic mail or Web sites to expedite transmission of voter registration materials and blank ballots. Readers are expected to consider this information within the framework of state and local election procedures and regulations. Only a basic understanding of information technology is required.

These best practices may also be useful to IT support staff charged with deploying, configuring, or maintaining the IT systems used to support the UOCAVA voting related activities described in this document, as well as system developers designing systems for these activities. As jurisdictions begin to deploy electronic delivery mechanisms alongside existing postal delivery mechanisms, previous decisions on appropriate policies and procedures for protecting election information may have to be reevaluated. This document identifies some of these issues that may come up when deploying a new system. As this document is primarily intended for election

officials, many technical details are left out of this document. The primary resource for technical computer security best practices is Draft NISTIR 7682 [2], along with NIST's existing collection of cyber security standards and guidelines.

## **1.4 Organization**

Section 2 provides an overview of the types of election materials that jurisdictions may wish to send to voters by electronic means, and describes what information is provided in this document to facilitate the secure and reliable transmission of those materials to overseas and military voters. It also provides high-level descriptions of the two Internet-based transmission methods that are considered in this document, electronic mail and Web sites.

Section 3 discusses security best practices for sending or receiving voter registration and ballot request materials via fax, electronic mail or Web sites. The section emphasizes the importance of protecting sensitive personally identifiable information that may be recorded or stored by the system, and discusses items that jurisdictions should consider on the issue of voter authentication.

Section 4 covers security best practices for using fax, electronic mail and Web sites to deliver blank ballots to overseas and military voters. The section discusses issues that jurisdictions must consider before deploying electronic ballot delivery systems, including ballot control and tracking, and if voter authentication is required prior to serving ballots. This section also considers the use of e-mail to deliver printable ballots, posting blank ballots on Web sites for voters to download, and the use of online ballot markers.

This document includes two appendices that provide an election officials and staff with an introduction to key computer security processes. This information is similar to the material covered in Draft NISTIR 7682, but written for election officials rather than system administrators and IT staff. A basic understanding of these processes will help election officials manage their staff, and ensure that policy decisions are made and key activities are performed by the proper staff members. Appendix A provides a brief overview of general computer security best practices that jurisdictions should follow, mainly from a process perspective. Appendix B provides an overview of technical controls for protecting IT systems used to support UOCAVA voting.

## 2 Overview

### 2.1 Types of Election Materials

Electronic transmission methods can be used to deliver election materials at all stages of the election process. This section outlines different types of election materials that jurisdictions may wish to deliver to their uniformed and overseas voters using fax, electronic mail or Web sites, and highlights some issues regarding security controls needed to keep information confidential and unmodified.

#### 2.1.1 Dissemination of Election Information Materials

Jurisdictions often make announcements reminding voters of upcoming elections, or asking them to ensure their voter registration information is up to date. They may also disseminate sample ballots and information explaining questions that will appear on the ballot, such as a bond issue.

The same message may be provided to all voters. In such cases, the information in the announcement is considered public information and therefore is not sensitive. This document will not discuss best practices for the distribution of these election information materials. However, ensuring the availability and reliability of the systems used to disseminate this information is important, and jurisdictions are directed to NISTIR 7682, *Information System Security Best Practices for UOCAVA Supporting Systems* [2], for information on security best practices to guard against accidental or malicious threats to system availability.

In some cases, announcements to voters may be personalized, particularly in the case of personalized e-mail messages to registered voters. For instance, an e-mail requesting that UOCAVA voters update their voter registration information may be personalized with the mailing address on file for each voter. Such communications should be treated as any other transmission of voter registration materials (see Section 2.1.2 for further discussion on voter registration and ballot request). In other cases, jurisdictions should consider the sensitivity of the personalized information on each communication when determining if additional security precautions should be taken.

#### 2.1.2 Distribution and Receipt of Voter Registration/Ballot Request Forms

In most jurisdictions, overseas and military voters must register in the jurisdiction where they are eligible to vote absentee in order to be qualified to vote in future elections, although some jurisdictions waive registration for

military voters. A common method for voters to submit this information is the Federal Post Card Application (FPCA) [4], a standard federal form that all states are required to accept. In addition, each state has its own registration form that reflects its specific registration requirements. Both the state specific forms and the FPCA request the following information from voters: name, date of birth, sex, race, home address and political party preference. They also ask for various forms of contact information, including telephone number, fax number, e-mail address, and mailing address. The FPCA provides a field for a complete Social Security number and a field for a state driver's license number or other state identification number. The FPCA instructions for most states require only the last four digits of the Social Security number. This information is a matter of public record, and state law dictates both which fields may be shared upon request as well as how requestors may use that information. Both the FPCA and state specific forms typically require a wet signature. Signatures, Social Security Numbers and driver's license numbers are typically considered to be protected information that cannot be publicly released.

Blank FPCA and state specific registration and absentee ballot request forms are publicly available for downloading from multiple websites and do not require any special protections for electronic transmission. However, Social Security numbers, other official identification numbers, and original signatures require protection from unauthorized disclosure or modification when completed forms are being returned to jurisdictions either by mail or electronically. Section 3 will identify issues that jurisdictions should consider when evaluating the suitability of e-mail and Web-based return of these materials, and will discuss security controls that jurisdictions can implement to protect this information.

### **2.1.3 Blank Ballot Delivery**

Because electronic transmission does not suffer from the same delays associated with postal mail delivery, e-mail or Web-based delivery of blank ballots can significantly reduce the round-trip transit time. Postal mail delivery to overseas locations can take significantly more time than delivery times within the United States. For example, one-way delivery through the military postal system to Middle East post offices takes at least 7-12 days [5]. Then the mail piece may have to be forwarded to the recipient's actual location, further increasing the transit time to the voter.

Blank ballots typically do not contain any sensitive information that must be protected from disclosure to third parties. However, care should be taken that ballots are reliably delivered to voters without unauthorized modification that could invalidate voters' cast ballots. Section 4 will discuss procedures

and technical controls that jurisdictions can use to help ensure safe transmission of ballots.

Blank ballots may be accompanied by additional personalized information on the voter affidavit or the ballot return envelope. This information often takes the form of a bar-coded voter identification number, which can help jurisdictions process returned ballots more efficiently by partially automating some of the data entry steps. Some commercially available systems allow jurisdictions to send out ballots with tracking information on return envelopes or ballots. This type of return identification information is usually non-sensitive, and does not require protective mechanisms to ensure confidentiality. However, this information may benefit from integrity protections, depending on how jurisdictions will use this information. Section 4.2 discusses issues that jurisdictions should consider when employing these mechanisms to track and identify ballot materials.

## **2.2 *Electronic Delivery Options***

Information can be quickly and easily transmitted electronically between parties by using fax, e-mail or posting information on Web sites. While e-mail and web sites both use the same underlying communications infrastructure, the public Internet, there are important distinctions between the ways these two technologies work, and how they might be used to transmit election materials.

### **2.2.1 Fax**

Many jurisdictions use fax machines to send or receive absentee voting materials. Fax machines scan a document and transmit an encoded representation of it over the telephone network to another fax machine. The receiving fax machine can decode the information and print a copy of the scanned document. Current fax machines create a digital representation of the scanned document. The digital representation is then sent over the telephone network using analog signals.

There is no widely-used standard for fax encryption. Thus, information sent by fax is at risk for possible interception or modification. Jurisdictions should carefully weigh the risks of fax transmission of election materials against the possible alternatives prior to using fax to send or receive sensitive information.

There are some Internet-based fax service providers that allow users to send or receive faxes over the Internet, using web sites or e-mail to send or receive faxes. These services have complex security properties depending



on how they are implemented or used. This document assumes jurisdictions using fax to send or receive election information will be using traditional fax machines directly connected to a phone line. However, jurisdictions cannot prevent voters from using these online services if they accept materials by fax.

## **2.2.2 Electronic Mail**

### **2.2.2.1 Overview and Description**

E-mail allows an individual to send text and/or files from one computer to another. E-mail is transmitted from the sender's computer to his or her mail server (often operated by his or her Internet Service Provider (ISP)), and routed through a series of intermediate servers and Internet routers before being delivered to the recipient's mail server (often operated by an ISP, workplace or a commercial e-mail service provider such as Gmail or Yahoo).

An e-mail sent from an election official passes through the jurisdiction's e-mail server, which is typically under the control of the local jurisdiction. The e-mail passes over the Internet, typically unencrypted, to a server controlled by the voter's e-mail service provider. In many cases, e-mail must pass through the public Internet once again to reach the voter, as many users have e-mail hosted by someone other than their Internet Service Provider (ISP). This connection may or may not be encrypted, depending on the voter's e-mail provider.

Just as mailed forms and ballots may be lost or delivered to a no longer valid address, e-mailed materials may not reach the intended voter. In many cases, senders will receive notification if the e-mail server of the recipient does not accept the message. Such an error may happen if the e-mail account is no longer active. However, just as election officials have no way of knowing if voters open election-related mail, they have no way of verifying that e-mails have been read by voters. While some e-mail clients support read-receipts, which are a way to request that the recipient send notification to the sender when an e-mail is read, these receipts are not widely supported in web-based e-mail clients and individuals typically must opt to send a reply. Consequently, the usefulness of read receipts for delivery confirmation may be limited.

As commonly implemented, e-mails are typically sent without cryptographic protections such as encryption or signing. As such, e-mails may be intercepted, read, and potentially modified as they are sent between election officials and voters. This is similar to the threat of mailed registration materials and ballots being delivered through the postal mail, which also has limited protective mechanisms. A key difference between these threats is

scale; an individual with the necessary technical skills may be able to intercept a large number of e-mails, while relatively few postal workers may be in a position to intercept a large number of mailed election materials. E-mail appears relatively more vulnerable to interception of messages compared to postal mail, where there are well-established legal penalties for tampering or intercepting mail.

Election officials considering the use of e-mail transmission of election materials should carefully consider the security limitations of e-mail and the availability of alternative delivery methods. Sensitive information sent over e-mail could be intercepted, read, and modified in transit. Sensitive information should not be sent over e-mail when suitable alternatives are available. E-mails can be easily forged to make it look like it was sent from another individual. These threats are not unique to e-mail, but could potentially be done on a larger scale than was possible with election materials mailed through the postal system. Election officials should consider the sensitivity of the information, the level of risk that it could be intercepted or modified, and the availability of suitable alternative delivery methods before using e-mail to transmit election materials.

- **Registration and Ballot Request Materials:** A typical application of e-mail in the UOCAVA voting process is to e-mail attachments (see Section 2.2.2.3) containing blank voter registration forms to voters (e.g., FPCAs), or receive completed forms from voters. Section 3.4 describes security best practices for e-mail transmission of voter registration and ballot request materials.
- **Blank Ballots:** E-mail is currently being used by many jurisdictions to send blank ballots to voters. Section 4.4 describes security best practices for e-mail transmission of blank ballots.

#### 2.2.2.2 E-mail Error Messages

Incoming and outgoing mail servers may send error messages to the e-mail sender or originator in the event of some type of error. These take the form of e-mails from the sender or recipient's e-mail server. Election officials that send e-mails to voters should be familiar with typical e-mail error messages, but the absence of an error message does not necessarily mean that an e-mail was properly received by the intended recipient.

E-mails can fail to be properly delivered to a recipient for a variety of reasons. These include:

- The intended recipient's e-mail address is not recognized (e.g., the intended e-mail account does not exist, the address was mistyped, etc.).

- The outgoing e-mail server is unable to send e-mails due to a loss of communications or a malfunction.
- The recipient's e-mail server cannot be contacted.
- The intended recipient's e-mail folder is full, and the server will not accept additional e-mails.
- The outgoing e-mail server, or the recipient's e-mail server, detected a virus or classified the e-mail as spam.
- The e-mail is too large (e.g., due to a large attachment) for either the outgoing e-mail server, or the recipient's e-mail server.

Election officials should read error e-mail messages in their entirety to determine what additional steps to take. For instance, if the outgoing or recipient's e-mail server is down temporarily, the issue may be resolved on its own. However, if the error message indicates that a message was not delivered, the official should attempt to identify the source of the problem. The error message may reveal a technical problem that can be remedied, such as a problem with the e-mail server or a simple mistake, allowing the e-mail to be resent. If the problem cannot be remedied, election officials should apply the same procedures used by the jurisdiction when it has evidence that a mailed ballot did not reach its destination.

Election officials should be aware that some e-mail error messages are sent to the intended recipient, not the sender. For example, if an e-mail is filtered by the recipient's e-mail server due to a detected virus, often that server will only send the error message to the recipient.

### **2.2.2.3 Attachments**

E-mail messages are text-based, but can include one or more files as attachments. While text-based e-mails are usually relatively small, e-mails containing attachments can be quite large. Depending on the attachment, an e-mail could become large for the sender's or recipient's e-mail server. In most cases, e-mails under 2MB) will be transmitted and accepted by e-mail servers.

E-mail servers often scan attachments for viruses, and some e-mail servers will reject e-mails containing attachments of certain file types that often contain viruses. In most cases this should not be an issue for jurisdictions, as typical file types (e.g., .DOC, .PDF, .RTF, .JPG) will be accepted.

### **2.2.2.4 E-mail Encryption and Signing**

E-mail can be cryptographically protected using encryption or digital signatures. E-mail encryption protects e-mails from being read by unauthorized parties, while e-mail signing allows recipients to verify the origin and integrity of the message. The most widely-used standard for e-

mail encryption and signing is called Secure/Multipurpose Internet Mail Extensions (S/MIME) [7], which is described further in NISTIR 7682, *Information System Security Best Practices for UOCAVA Supporting Systems* and NIST SP 800-45, *Guidelines on Electronic Mail Security* [9].

Jurisdictions may receive digitally signed e-mails from UOCAVA voters, particularly from military voters using their Department of Defense e-mail accounts. The contents of these e-mails can generally be read without any specific e-mail software, but additional measure must be taken to verify the digital signatures on these messages. Jurisdictions that wish to verify the signatures from military voters need to use an e-mail client that supports S/MIME and will need to install the trust anchor for the US Department of Defense Root Certificate Authority. Configuring e-mail clients to receive and verify S/MIME signed e-mails is covered in Section 5 of NISTIR 7682.

Jurisdictions could also digitally sign messages they send. This also requires an e-mail client that supports S/MIME, which must be configured with a cryptographic key and a certificate that binds that key to the jurisdiction. Certificates can be purchased from commercial Certificate Authorities (CA), although only some of them issue certificates for S/MIME. Some states also run their own Certificate Authority. However, signing e-mails is only beneficial if voters have a properly-configured e-mail client that supports S/MIME, expect to receive signed emails, and know how to use the client to verify the signatures on those e-mails. As signed e-mails are not common outside of the military environment, this may not be true for overseas civilians or military personnel using personal e-mail accounts. Jurisdictions that still wish to sign e-mails should consult Section 5 of NISTIR 7682.

#### **2.2.2.5 DomainKeys Identified Mail**

The Internet Engineering Task Force recently completed a suite of standards for DomainKeys Identified Mail (DKIM) [10]. DKIM is a limited form of e-mail authentication that allows a jurisdiction's e-mail server to sign outgoing messages so other DKIM-aware e-mail servers can verify the integrity and origin of the message. This is typically used to protect against unsolicited e-mails, also known as spam. Individuals sending spam sometimes forge e-mails to trick recipients or to try to avoid e-mail spam filters. DKIM provides a mechanism for detecting forged e-mails, but only when the receiving e-mail server and the e-mail server for the (possibly forged) organization support DKIM.

Use of DKIM by jurisdictions' e-mail servers can help to reduce the chances that their outgoing e-mails will be marked as spam by recipients, and could help to improve their own e-mail filtering systems for spam and malware.

Current best practices for jurisdictions include using DKIM to sign outgoing mail and have DKIM-aware servers to process e-mails to protect themselves from spam and malware, but should not rely on DKIM to verify the original senders of e-mails. Accepted best practices will change over time as DKIM is more widely adopted.

## **2.2.3 Web-Sites**

### **2.2.3.1 Overview and Description**

Web sites are a popular method for posting information so that anyone with a Web browser can access it. Web sites can be used to host election information, voter registration forms, or blank ballots. Some jurisdictions have also used web sites to allow voters to submit voter registration information.

While e-mails could be lost or delivered to an invalid address, web sites allow voters to instantly access information at-will. While web sites could become unavailable due to technical difficulties or malicious attacks, they do not suffer from some of the potential delivery problems as postal mail or e-mail.

However, just as with postal mail and e-mail, communication between a voter and a web site could be intercepted, read, or potentially modified in-transit. Wide-deployed cryptographic protections, such as Transport Layer Security (see Section 2.2.2.4) could be used to guard against many of these attacks. However, there are less sophisticated, but often just as effective, attacks that attempt to trick users into accessing the wrong web site. For example, a typical attack on the Internet called Phishing involves tricking a user into clicking on a link to a fraudulent Web site that closely mimicks the legitimate site, such as copying the jurisdictions' logos. Such attacks are very difficult to block by technical means, but can be mitigated through awareness training.

### **2.2.3.2 Online File Repositories**

Web sites may be used to host election-related documents, such as voter registration and ballot request forms (e.g., FPCA) or blank ballots. These sites could be available for all visitors to the site, or access to these forms may be controlled so that only users with a password, or some other authenticator, can access the forms. While Web sites may be more expensive to deploy and use than e-mailing election materials, they do have several advantages. Notably, there are greater security protections possible for delivery of materials over Web sites than over e-mail (see Section

2.2.3.4). Security best practices for posting forms and other information on Web sites will be discussed in Sections 3.5.1 and 4.5, respectively.

It is also possible for users to upload files to a Web site, as an alternative to e-mail. Again, an advantage to this approach is that Web-based transmission is easier to protect than e-mail transmission. Receiving voter registration or ballot request forms over Web sites will be discussed in Section 3.5.2.

### **2.2.3.3 Sites with Active Content**

Rather than merely posting static Web pages or documents, Web sites often include active content that run as a sort of application in users' browsers. This could take the form of a Web-based form and javascript where a voter enters information, or a Java or Flash-based application that is downloaded by a voter's browser and executed within the browser window.

For example, a Web site supporting voter registration and ballot request could have a Web-based form that allows voters to enter their registration and contact information, and submit it to the election officials. Often Web-based forms will include some logic that advise users of mistakes, such as omitting required information such as an address or phone number. These sorts of forms are a staple of e-commerce Web sites. These forms could also be used for online ballot marking, allowing voters to record their selections on the form before printing the voted ballot for return through the mail.

Section 3.6 contains security best practices for receiving voter registration or ballot request information using Web sites with active content. Section 4.6 contains security best practices for using these technologies to allow voters to receive and mark a ballot electronically.

### **2.2.3.4 Transport Layer Security**

Transport Layer Security (TLS) [14], and its predecessor, Secure Socket Layer (SSL), are cryptographic protocols that provide confidentiality and integrity protection for communications between a Web server and a client accessing that server. TLS and SSL are widely used on the Internet to provide a safe communications channel for sending sensitive information. For instance, nearly all e-commerce Web sites use TLS to protect any financial or transaction information sent between the server and user.

TLS is typically used with only server-side authentication, meaning that users connecting to a Web site can verify that they are communicating with the intended entity, but the Web server does not cryptographically verify the users. To be effective, TLS-enabled Web servers must have a public key

signed by a commonly-trusted certificate authority. There are a number of commercial vendors for TLS certificates. However, while TLS is capable of verifying the identity of users (typically called client-side authentication), this requires users to have a public key signed by a trusted certificate authority. This typically is not the case.

TLS is an inexpensive, widely deployed and supported technology, which should be employed by any Web server that sends or receives sensitive information.

## **2.3 Cryptography**

Cryptography is the use of mathematical and computer algorithms to protect the confidentiality or integrity of information as it is stored or transmitted.

Most cryptographic algorithms fall into one of two classes:

- Encryption algorithms for protecting the confidentiality of information in-transit or in storage.
- Message authentication codes or digital signatures for establishing trust in the authenticity and integrity of information.

Cryptographic algorithms are used in cryptographic protocols to provide the intended security properties. These protocols often combine several different algorithms to provide confidentiality and integrity protections. Proper use of cryptography is critical to the protecting information in computer systems. Previous sections gave some examples of the use of cryptography to protect information as it is transmitted over the Internet: e-mail encryption and signing, and the SSL/TLS protocol for protecting web sites. This section provides additional background information intended to give readers a better understanding of how cryptography can be used to protect information in UOCAVA voting systems.

### **2.3.1 Cryptographic Confidentiality Protections**

Encryption algorithms are cryptographic algorithms that aim to protect the confidentiality of information. These algorithms scramble (encrypt) information so that it can only be unscrambled (decrypted) and read by someone with the correct key, which must be kept secret. Encryption algorithms might be used on stored data in computer systems to help ensure sensitive information is not read by unauthorized individuals. Or it might be used to protect information that is transmitted over the Internet so eavesdroppers are not able to read the data.

Most encryption algorithms fall into one of two categories: symmetric encryption and asymmetric encryption.

- **Symmetric encryption algorithms** use a single secret key to encrypt and decrypt information. For that reason, it is sometimes called secret key encryption. It is most often used to encrypt information that is stored locally on a machine, or to protect information that is transmitted between two different parts of a single system. Proper key management is particularly important when using symmetric encryption algorithms. The key must be securely stored. If a symmetric encryption algorithm is used to protect information sent between two computers, users must securely load the same key on both systems, usually by manually loading the key. The two government standards for symmetric encryption algorithms are the Advanced Encryption Standard (AES) and the Triple Data Encryption Standard (TDES).
- **Asymmetric encryption algorithms** use two different keys: one key to encrypt data, and one key to decrypt data. The key used to encrypt data is the public key, and can be shared with anyone. The key used to decrypt data is the private key, and must be kept secret. Because the encryption key can be freely shared, asymmetric encryption algorithms are often easier to use when two parties are communicating over the Internet. Asymmetric encryption algorithms are rarely used to encrypt content directly. Asymmetric encryption algorithms are usually used to encrypt a new key. This new key is used in a symmetric encryption algorithm to encrypt the actual content. Asymmetric encryption algorithms include algorithms such as RSA and Diffie-Hellman, and are frequently used in electronic commerce.

### 2.3.2 Cryptographic Integrity Protections

There are several different types of cryptographic algorithms that can be used to protect the integrity of information. Notably, these include digital signatures and cryptographic message authentication codes. These algorithms primarily provide two security properties. First, they allow users to verify that the information was not changed. Second, they allow users to authenticate the originator of the information.

- **Digital Signature algorithms**, like asymmetric encryption algorithms, use two different keys. One key is used to sign data, while the other key is used to verify signatures created using the first key. The key used to verify signed data is the public key, and can be shared with anyone. The key used to sign data must be kept secret to prevent other people from forging signatures. Digital signatures are used in many applications to provide integrity protection and to authenticate users and information.



- **Message Authentication Codes**, like symmetric encryption algorithms, use a single secret key to compute and verify cryptographic fingerprints. These fingerprints are somewhat similar to signatures, except only someone that knows the secret key can verify the tag. Message authentication codes are frequently used to protect information that is transmitted over the Internet from manipulation.

### 2.3.3 Cryptographic Protocols

Cryptographic algorithms are used as building blocks in cryptographic protocols. These protocols usually use a combination of cryptographic algorithms to provide a combination of confidentiality and integrity protections. For example, the S/MIME protocol uses digital signature algorithms and both symmetric and asymmetric encryption algorithms to encrypt e-mails, sign e-mails, or encrypt and sign e-mails. The TLS protocol uses all four types of cryptographic algorithms previously described to protect the confidentiality and integrity of data transmitted between users and web servers.

### 2.3.4 Digital Certificates

Digital signatures and asymmetric encryption are examples of public key cryptography. These types of cryptographic algorithms require that its users have a private key that must be kept secret, and a public key that can be freely shared without a loss of security. However, there needs to be a way to securely bind the identity of a user or system to a specific public key, otherwise users would not know what public key to use when communicating with another user.

This kind of binding is done with a digital certificate. A certificate is a record with several fields. The most important of these fields include:

- *Identifier*: This field (or fields) identifies the person or system that "owns" the certificate. This person or system is known as the "subject." For SSL/TLS, it may be a web site address. For S/MIME it may be an e-mail address. In other cases it might just be a name.
- *Public Key*: This field contains the subject's public key that other users should use when decrypting messages or verifying digital signatures.
- *Algorithm Use*: This field describes what algorithms or protocols may be used with the digital certificate.
- *Expiration Date*: Most certificates expire after a set period of time. The duration of the certificate will depend on a number of factors, including the strength of the cryptographic algorithm and key, how the certificate will be used, and the cost of the certificate.

The information in digital certificates is digitally signed by a certificate authority. This signature is the certificate authority's way of attesting that the individual (or system) in the identifier field is the true owner of the public key found in the certificate.

Which systems require digital certificates depends upon the particular cryptographic protocol. For example, web servers using TLS/SSL need a digital certificate from a trusted certificate authority, but users who access the web site do not need to obtain their own certificates (unless the server is also cryptographically authenticating users, which is sometimes done in high-security systems). A user signing an e-mail using S/MIME must obtain a digital certificate. Signed e-mails from the user contain a copy of this certificate, allowing recipients to verify the signature. However, recipients must trust the certificate authority who issued the certificate.

### **2.3.5 Certificate Authorities**

Certificate authorities are trusted third-parties that vouch for the validity of an individual's certificate, asserting that the individual or system identified in the certificate is the "true" owner of the public key identified in the certificate. The receiver of a signed message, or the sender of an encrypted message, must trust the certificate authority that issued the certificate used in the transaction.

For the applications of cryptography outlined in this document, there are primarily two ways to obtain widely trusted digital certificates. The most common way is to purchase one from a commercial certificate authority. There are several commercial certificate authorities that sell digital certificates. Jurisdictions should be careful to purchase certificates from authorities that are widely trusted by their targeted systems. For example, if a jurisdiction is purchasing a digital certificate to enable the use of TLS on a web server, the jurisdiction should ensure the issuing certificate authority is trusted by all major web browsers that voters may use to access the web site.

Alternatively, some states may run their own certificate authority. State and local jurisdictions may also be able to obtain and use certificates from these authorities, particularly if the state's certificate authority is affiliated with the federal government's certificate authority. Again, jurisdictions will need to ensure the certificate authority is widely trusted by applications that may use the system.

Jurisdictions will also need to ensure that they obtain the right kinds of certificates. A certificate used for S/MIME e-mail signing cannot be used to

digitally sign documents, or implement TLS on a website. Certificate authorities usually do not issue certificates for all types of applications.

While the costs of obtaining certificates can add up if a large number of certificates are needed for a large number of systems or users, the applications of cryptography identified in this document will typically not require such large deployments. In most cases, jurisdictions will only need to purchase a very small number of certificates to make use of TLS on web servers or to sign documents.

## **3 Transmission of Registration/Ballot Request Materials**

### **3.1 Overview**

Voter registration and requests for a blank ballot by the UOCAVA voter can be reliably facilitated and expedited by the use of any of the electronic transmission options discussed in this document, including transmission over e-mail and Web sites. Voter registration applications and absentee ballot request forms, such as the Federal Post Card Application, are frequently available on websites and transmitted to voters by fax or e-mail. As public forms, these materials do not need confidentiality protections, but could benefit from technical controls aimed at ensuring the integrity and availability of these forms. However, completed voter registration or ballot request forms can contain sensitive information, and improper protection of these forms in transit, storage and processing can put this information at risk of theft or manipulation. Failure to securely transmit these forms to election officials could impact the ability of voters to obtain ballots. This section will cover basic procedural and technical security controls aimed at protecting information related to voter registration and blank ballot request materials.

### **3.2 General Issues**

#### **3.2.1 Voter Registration**

Once an applicant is determined to be a qualified voter in a jurisdiction, the voter registration process implicitly establishes a trusted relationship between the applicant and the jurisdiction. The voter registration process may establish a trusted authentication token that is used to authenticate future correspondence from the voter. For instance, the voter's signature on a voter registration form may be used to authenticate received absentee ballots, or updates to the voter's registration information. Systems used for UOCAVA voting may require the voter registration process to establish electronic authentication tokens, such as a password or cryptographic key.

State law may prohibit receiving voter registration forms via electronic methods. For instance, some state and local jurisdictions require that the voter registration form have an original hand-written signature, often called a "wet" signature. In these cases, faxed or scanned registration forms sent over e-mail or web sites would not be allowed.

The move to electronic or online voter registration may require changes to the process of establishing this authentication token, as allowed by state law. For example, some states and local jurisdictions now have the ability to

use signatures from Department of Motor Vehicle records to authenticate election correspondence.

Jurisdictions that are unable to accept electronically transmitted voter registration materials may still be able to accept electronically transmitted materials for updating voter registration information, or requests for blank ballots.

### **3.2.2 Voter Authentication**

State law will determine appropriate authentication mechanisms for accepting voter registration materials, blank ballot requests, and returned marked ballots. This includes the initial authentication and identity-proofing information to verify an individual's voter registration materials and eligibility to vote, as well as any subsequent correspondence between the jurisdiction and the voter, such as updates to mailing addresses or returned marked ballots.

Most state and local jurisdictions primarily use voters' signatures to authenticate voter registration forms and returned marked ballots. In these cases, election officials use the signature from the voter's file to authenticate correspondence. The signature on file might be from the voter's initial voter registration form, or it may be a signature from other state records, such as Department of Motor Vehicle (DMV) records.

The move to electronic transmission methods may require the use of alternative authentication mechanisms, particularly in cases where voters are allowed to submit information electronically. For example, some state and local jurisdictions allow voters to register to vote, request blank ballots, or change their voter registration information online. Digitized voter signatures may not be a viable or desirable option for voter authentication for these types of systems. Local election officials should consult state law to determine what forms of electronic authentication are required or allowed in their jurisdictions.

Identification numbers, such as the social security, drivers' license, or passport number, are sometimes used in online voter registration or ballot delivery systems for voter authentication. However, these identifiers, while forms of sensitive information, have limited strengths as authenticators. Social security numbers are known by many parties other than the holder, and in some states driver's license numbers are merely an encoding of the holder's name and date of birth. Jurisdictions should carefully consider the use of these identification numbers as authenticators.

E-mail return addresses and headers cannot be used for voter authentication purposes. As noted in Section 2.2.2, this information is very easy to forge.

### 3.2.3 Protecting Personal Voter Information

Voter registration applications and absentee ballot requests contain personally identifiable information, such as names, addresses, and identification numbers. The Government Accountability Office defines personally identifiable information (PII) as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”[24] Election authorities should consult relevant state and local laws to review relevant rules and regulations governing the use and protection of PII and voter registration information in their jurisdiction.

Voter registration information is a matter of public record, but state law may limit public distribution of some categories of information, such as identification numbers (e.g., Social Security, driver’s license, and passport numbers) and, in some cases, home addresses. State law may also limit acceptable uses of information obtained from voter registration records, and force individuals requesting this information to take an oath affirming compliance with relevant laws. Jurisdictions should consider any relevant legal and procedural controls in place for protecting PII in voter registration records when determining appropriate technical and procedural controls for this information in electronic systems.

Not all PII must be protected equally. Public availability of the data is just one item to consider when determining an appropriate level of protection for PII and voter registration information. Section 3 of NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, identifies six factors that organization should consider when determining the appropriate level of protection. Organizations should consider the following:

- How easily the PII can be tied to specific individuals.
- The number of individuals whose PII is stored in the system.
- The sensitivity of the data.
- The context of how the data will be used, stored, collected, or disclosed.
- Legal obligations to protect the data.
- The location of the data, and level of authorized access to the data.

Further guidance on what constitutes PII, factors that influence PII sensitivity, and how PII should be handled from collection to destruction is provided in NIST SP 800-122 [25].

Highly-sensitive forms of PII should not be sent over the Internet without use of encryption technology. After consulting local, state and federal law, jurisdictions must determine what constitutes sensitive PII, or whether the factors provided above indicate that a given set of PII may or may not be sent over the Internet without encryption or integrity protections, erring on the side of caution when possible. However, it is relatively easy and inexpensive for jurisdictions to encrypt information in-transit to and from Web sites using TLS.

### **3.2.4 Preparing Registration/Ballot Request Forms**

Voter registration forms that are intended to be e-mailed or posted on Web sites should be converted into a publicly-available document format. For example, many jurisdictions use the Portable Document Format (PDF) [21].

Notably, forms should not be merely electronic scans of paper documents. Electronically scanned documents are typically much larger than documents directly saved in an electronic document format, often contain text that is more difficult to read, and are typically not compatible with screen readers. Additional usability and accessibility issues are discussed in *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting* [23].

As noted in Section 3.2.3, forms developed by state and local jurisdictions for voter registration and ballot requests should not ask for information that is not required or desired by jurisdictions. State and county-specific forms should be designed to dissuade voters from filling in unnecessary information. When Federal forms, such as the FPCA, are used, the form should be accompanied with clear instructions for the voter identifying what information is and is not required.

Some publicly-available document formats support electronically-fillable forms, allowing voters to fill in the forms on their computers, even if they intend to print the document prior to return. Many formats have extensions that support scripting languages that can be used to help voters avoid mistakes when filling out forms. For instance, Javascript could be used in the PDF format to warn voters if they miss required questions. However, these extensions can cause compatibility problems, and such documents should be tested in widely-used document viewers and introduce a variety of potential security vulnerabilities. In particular, jurisdictions using these extensions should ensure that the forms work even in document viewing

applications that do not support those extensions, or have these features disabled (e.g., Javascript may be disabled in many PDF readers for security reasons).

Some publicly-available document formats, such as PDF, support digital signatures. Jurisdictions may consider digitally signing voter registration or ballot request forms prior to e-mailing or posting them in order to give voters additional assurance that they received the correct, unaltered forms.

In order to sign documents, jurisdictions will need to obtain software packages capable of signing documents as well as a digital certificate from a certificate authority that is trusted in widely used document viewers. Usually a single certificate is all that would be needed. There are several commercial certificate authorities which sell certificates that can be used to sign documents, although these are less common than other types of certificates. State and local jurisdictions may also be able to use a certificate authority operated by the state, particularly if the state's certificate authority is affiliated with the federal government's certificate authority.

The benefits of signing documents should be weighed against the costs of obtaining the software and digital certificates necessary to support document signing, as well as the number of voters expected to be able to verify the digital signatures on signed documents. Most voters will not notice the difference between a signed document and an unsigned document, and in many cases signed documents are only verifiable using a document viewer from a particular software vendor. Users with other document viewers may still be able to open and view the document, but would not be able to verify the authenticity of the document. For those reasons, election officials may want to consult with other agencies in their jurisdiction to determine if another agency already has the requisite software and digital certificate to sign documents. If no other agency has these items, jurisdictions must decide whether or not the security benefit justifies the expense of the software and digital certificate.

### **3.3 Fax**

Jurisdictions should follow their standard procedures for ensuring voter registration and ballot request forms are correct before faxing them to voters. Election workers should take steps to ensure that disruptions or errors in the fax process are prevented or detected and resolved. If a jurisdiction accepts voter registration materials by fax, the fax machine should be kept in secure physical location to prevent the theft of sensitive personal information that may be on received voter registration forms.



Most fax machines keep a log of faxes that are sent and received. This includes successful and unsuccessful transmission. These logs may be useful auditing records to keep, but also could also allow voters' telephone or fax numbers to be disclosed to unauthorized parties if fax machines are not kept in secure locations, since these logs are usually available to anyone with physical access to the machines.

Some fax machines keep digital copies of sent or received faxes, often unbeknownst to users. These copies could put personal information on received voter registration forms at risk of disclosure to unauthorized individuals. Election workers should consult the documentation for the fax machines to determine if their fax machines store copies of received faxes. The documentation may also provide users with the steps needed to periodically erase this information.

### **3.4 Electronic Mail**

#### **3.4.1 Delivery**

Voter registration and ballot request forms should be prepared as described in Section 3.2.4 to ensure the electronic files have the best possible chance of being successfully delivered to voters. Jurisdictions should follow their standard procedures for ensuring these forms are correct before e-mailing them to voters.

Jurisdictions should beware of spam filters which may inadvertently mark their messages as spam and not display it to users. It is difficult to ensure that e-mails sent by jurisdictions will not be marked as spam. As previously noted, use of DomainKeys Identified Mail [10] on the jurisdiction's e-mail server may reduce the chances of outgoing e-mail being marked as spam. Jurisdictions may also consult the Message Anti-Abuse Working Group's *Sender Best Communications Practices* for additional technical measures [13].

E-mails should be addressed to voters individually, rather than sending a single e-mail to a group of voters. There are utilities and e-mail clients that can send the same message individually to a list of e-mail addresses. The "Reply-to" and "From" fields of the outgoing e-mail should be set to an e-mail account monitored by election officials. Election officials should closely monitor this e-mail account for any error messages that indicate a message was not properly received by the voter. Some types of e-mail error messages were described in Section 2.2.2.2. Election officials should read the error message to determine the nature of the problem and remedy it if possible, as it may be a sign of a technical malfunction. If the problem

cannot be remedied, election officials should apply the same procedures used by the jurisdiction when it has evidence that a mailed form did not reach its destination.

### **3.4.2 Reception of Forms**

Completed voter registration forms collected over e-mail are expected to be received and processed by election officials manually. As with e-mail delivery, workstations used to collect voter registration forms over e-mail should be configured according to accepted computer security best practices, such as using an encrypted connection to the e-mail server for both incoming and outgoing messages. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

As election officials will be opening e-mails from voters, and potentially attackers, it is important to properly secure the workstation against possible attacks. While these protections are appropriate for any election workstation, it is critical to ensure that the workstation is running up-to-date antimalware software at all times, and ensure that it is configured to scan incoming e-mail messages. Applications used to open e-mails, or to open e-mail attachments, should also be hardened. For example,

- Microsoft Office, and other document viewers, can be configured so that macros are disabled.
- PDF viewers may have configurable security protection mechanisms, and active content (e.g., javascript) can be disabled.

As discussed in Section 2.2.2.4, some voters may send e-mail messages signed using S/MIME. E-mail clients should be configured by IT staff to correctly process these messages. Most commercially-available e-mail clients include S/MIME functionality by default.

Election officials should develop appropriate procedures for handling and processing e-mails containing voter registration information. E-mail servers and clients are generally not suitable locations for storing sensitive information for extended periods of time. Election officials should process these e-mails as soon as possible, using their standard procedures for processing received voter registration forms. As part of this process, election officials may wish to save an electronic or physical copy of the received e-mail, including full e-mail headers and attachments, to the voter registration database or other voter management system. After processing, the e-mail should be removed from both the e-mail server and the e-mail client to prevent unauthorized access to any sensitive information on these forms.

Simply deleting e-mails from servers and clients does not typically remove all traces of those e-mails on those systems. Due to the way that e-mails are typically stored on servers and clients, file-level sanitization software cannot be relied upon to securely erase this data. These computer systems should be treated as any other containing potentially sensitive data, and sanitizing storage media prior to decommissioning or repurposing. Section 4.2.4 of NISTIR 7682 provides best practices for decommissioning systems.

### **3.5 Web-based Distribution and Reception of Forms**

#### **3.5.1 Delivery**

Voter registration and ballot request forms should be prepared as described in Section 3.2.4. Election officials should follow their standard procedures for ensuring these forms are correct prior to loading them on the server. Access control mechanisms should be used on the server to protect the forms from unauthorized access or modification. The server operating system and Web server application should be configured and deployed according to widely accepted computer security best practices.

Blank voter registration and ballot request forms, such as the FPCA, are public forms that do not require confidentiality protections. However, use of TLS or SSL can also protect the integrity of these forms as they are transmitted to voters.

#### **3.5.2 Reception**

Jurisdictions may receive completed voter registration forms over Web sites that allow users to upload the completed form to the jurisdiction's Web server. This approach offers greater security than e-mail transmission of voter registration and ballot request forms, notably encryption and integrity protection in-transit using SSL/TLS. However, these protections can also be used for Web-based forms, as described below in Section 3.6. In most cases, use of online forms will be preferable to uploading completed forms to a Web site, except in cases where a jurisdiction must obtain digitized voter signatures to authenticate received forms.

The Web server's operating system and election application should be configured and deployed according to widely accepted computer security best practices. For example files should be uploaded using the HTTPS protocol using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites. Uploaded files should not be stored directly on the Web server; rather, they should be received by the Web server, and stored on a system that is not directly accessible from the Internet. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

Jurisdictions should take steps to protect the availability of the online system. This includes ensuring the system has adequate capacity for the expected load, and contingency plans in the event of a service disruption. Jurisdictions may wish to implement technical controls in the repository to protect against attackers overwhelming the system. This could include the use of CAPTCHAs<sup>1</sup> to guard against automated attacks, or limiting the size of uploaded files.

Individuals could attempt to upload carefully crafted files as part of an attack. These files could contain malicious code or hidden instructions that could allow an attacker to take control of the system. Jurisdictions should implement security controls to reduce the likelihood that such files could successfully attack the system. For instance,

- The system could restrict file types users may upload to those commonly used for scanned documents. For example, a server could be configured to only accept commonly-used document or image file formats. This limits the ability of potential attackers to upload malicious code or other unwanted files, and makes it less likely that voters will upload the wrong file.
- The file type verification mechanism could read the contents of the file and verify the file format against the approved list of file formats, rather than only checking the file extension.
- The system could use access control mechanisms to ensure uploaded files are not readable, or executable, by the Web server. This will make it more difficult for malicious individuals to improperly access files uploaded to the server.
- Uploaded files could be sanitized and scanned for malicious code prior to making them readable by any other processes or users. All forms of user-input should be checked, including the file contents and the full file name. This important step attempts to protect workstations accessing these files from attacks involving malicious code.

Election officials should process uploaded forms as soon as possible, using their standard procedures for processing received voter registration forms. As part of this process, election officials may wish to save an electronic or physical copy of the received form. After processing, the uploaded form should be removed from the online system to protect against unauthorized access.

---

<sup>1</sup> CAPTCHA is an acronym for Completely Automated Public Turing test to tell Computers and Humans Apart.

### **3.6 Online Voter Registration Systems**

Jurisdictions may deploy Web sites that allow voters to view or submit voter registration and ballot request materials directly within the Web page. These systems typically work by allowing voters to submit information electronically to local election officials. Election officials process the submitted voter registration materials similarly to how they process voter registration forms received through the mail. The voter's record in the voter registration database is updated through this process conducted by the election official. In general, online voter registration systems should not automatically update voter registration information without direct involvement from an authorized election official.

Voters using the web site to register to vote or update their voter registration information will need to be authenticated. State law will determine appropriate authentication mechanisms. Depending on state law and the implementation of the system, voters may be authenticated prior to allowing them to submit information, or the system may allow anyone to submit information, with authentication performed by election officials during processing.

In most cases, it will be desirable to authenticate voters prior to allowing them to submit information. In these cases, the systems may authenticate voters using information stored in the voter registration database, as permitted under state law. For example, the system could ask the voter to provide some difficult-to-guess information that can be verified against existing voter registration information. Because this is a relatively weak form of authentication, measures should be taken to protect against malicious users submitting fraudulent information by correctly guessing the information used for authentication purposes.

For instance, multiple consecutive invalid authentication attempts should result in the voter's account being temporarily locked, preventing further access attempts, for a predefined period of time (e.g., 24 hours) or until the case can be reviewed by an election official. The number of allowable invalid authentication attempts should be dependent on the difficulty of guessing the required authentication information. If information is relatively easy to guess, such as the voter's registered zip code or date of birth, is used for authentication purposes, then a lower number of invalid authentication attempts could be used. Information that is more difficult to guess, such as an identification number that was generated randomly by the issuing authority, may allow a higher number of invalid authentication attempts to be used.

If voters are not authenticated prior to allowing them to submit information to the online voter registration system, the system should use other mechanisms to attempt to prevent automated attacks whereby an attacker submits a large number of invalid registration changes or ballot requests. An example from e-commerce sites is the use of a CAPTCHA to block automated attacks. CAPTCHAs are little puzzles that users are asked to solve, often involving reading distorted text, to prove that a human is accessing a Web application. CAPTCHAs are often used to try to block attacks where automated computer programs access a Web site and attempt to submit or collect information.

Voters should be authenticated prior to showing them any sensitive voter information. In general, highly sensitive data, such as driver license numbers, passport numbers, social security numbers, and other identification numbers, should not be presented to voters. Non-sensitive information, such as publicly-disclosable information from voter rolls, might be viewable with limited or no authentication performed. In these cases, jurisdictions should consider implementing controls to prevent an individual from collecting large amounts of information in an automated fashion, such as using CAPTCHAs.

The Web server's operating system and the election application hosting the vote registration and ballot request form should be configured and deployed according to widely accepted computer security best practices. For example, the Web site should be hosted using the HTTPS protocol using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites. Information submitted using the form should not be stored directly on the Web server; rather, it should be received by the Web server, and stored on a system that is not directly accessible from the Internet. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

Making voter registration materials available online may create some privacy concerns. Jurisdictions should carefully consider the advantages and disadvantages of deploying such systems. A report issued by the National Research Council, *Improving State Voter Registration Databases* [27], discusses some of the policy and security issues in Appendix D that can be considered prior to deploying online voter registration systems.

## **4 Delivery of Blank Ballots**

### **4.1 Overview**

As noted in NISTIR 7551, blank ballot distribution to overseas and military voters can be reliably and securely expedited by using electronic transmission methods, including electronic mail and Web sites [1]. Several states and jurisdictions deliver ballots electronically to overseas and military voters, usually by sending these ballots as e-mail attachments. Security best practices for e-mail transmission of blank ballots are provided in Section 4.4. However, e-mail offers limited confidentiality and integrity protection in-transit, as the required infrastructure to support e-mail encryption and digital signing technologies are not widely deployed or used by the general population. Web-based methods can provide greater confidentiality and integrity protections by using SSL or TLS. Web sites could be used to allow voters to download ballot documents that can be printed and marked by hand, or they provide voters with a Web-based application that can allow voters to make their ballot selections on a computer, and print a marked ballot containing their selections. Best practices for these methods are discussed in Sections 4.5 and 4.6, respectively.

### **4.2 General Issues**

#### **4.2.1 Voter Identification and Authentication**

State law will determine if jurisdictions must authenticate voters prior to sending them blank ballots, or if jurisdictions need to only authenticate returned marked ballots. It is important to distinguish voter authentication from voter identification. Web-based ballot distribution systems need to request sufficient information from a voter to identify the appropriate ballot style. If the information requested is not secret, and is primarily intended to identify the correct ballot style, rather than to restrict access to electronic ballots, it should not be considered an authentication mechanism.

However, for Web-based ballot distribution systems, state and local jurisdictions may still decide to employ systems to authenticate voters before serving them ballots, as allowed by state law. For example, a UOCAVA voting system might distribute blank ballots with return identification information on the voter affidavit that is used to assist election officials when processing return ballots. If this information is used to establish trust that a given ballot was completed and returned by the claimed voter, the system will need to authenticate voters electronically prior to giving them ballots and voter affidavits.

In most cases, any mechanism used to remotely authenticate voters will serve as a secondary method to authenticate returned ballots, with voter signatures generally providing the primary mechanism to authenticate returned ballots. As such, the strength of the remote authentication method can be relatively weak as long as jurisdictions are confident in their ability to verify voter signatures.

#### **4.2.2 Ballot Accounting**

As part of the ballot accounting process, many jurisdictions keep track of the total number of ballots printed to detect fraud and to audit the election process. Once ballots leave the control of a polling place environment, however, ballots can be copied, limiting the effectiveness of these checks. Printing ballots on special ballot stock provides some level of protection against copying mailed ballots, but electronically transmitted ballots are easy to copy and transmit to third parties.

Jurisdictions that are particularly concerned about unauthorized copying of electronic ballots may put cryptographically integrity-protected identifiers on each transmitted ballot that would uniquely identify a given ballot. For example, a ballot serial number could be digitally-signed or protected using a cryptographic message authentication code. While these ballots could be copied, a third party could not create a new ballot with a different identifier, as the third party could not create a valid digital signature on that identifier. However, placing unique identifiers on ballots introduces potential problems related to ballot secrecy. Jurisdictions should consult relevant state law to determine if such protections are appropriate or allowable.

A possible alternative to placing unique identifiers on each ballot is to cryptographically integrity-protect return identification information that must accompany ballots when they are returned, but are separated from the ballots before tallying. This method provides a similar level of protection against unauthorized individuals returning copied electronic ballots.

However, jurisdictions may still find it desirable to place identifiers on ballots in order to track ballots from distribution to tallying. Such identifiers could assist election officials during the ballot reconciliation process. The advantages and disadvantages to using these types of identifiers are discussed in Section 4.2.4, *Ballot Tracking*.



### 4.2.3 Return Identification

In order to correctly process completed ballots upon return to a voter's local election office, completed ballots are accompanied with return identification information that identifies (e.g., voter name, voter identification number) and authenticates (e.g., voter signature) the voter. The information identifying the voter may be written by the voters themselves, or it can be pre-generated on the materials provided to voters. In the case of postal mail voting, this information is usually printed on the ballot return envelopes that are delivered to voters with blank ballots. In the case of electronic distribution of ballots this information would likely be printed on sheets of paper that would accompany a completed ballot.

Computer-generated return identification information, whether created by election officials prior to transmission of blank ballots, or by software on voters' machines (e.g., java or javascript running in a browser), can be machine-readable, in the form of barcodes or text printed in a font compatible with optical character recognition. Any machine-readable return identification information should also be available in human-readable form as well, except for information intended to protect the integrity of the machine-readable encoding (e.g., digital signatures, checksums, message authentication codes, or error correcting codes).

As noted in Section 4.2.1, return identification information is usually used as a secondary voter authentication mechanism, with voter signatures serving as the primary authentication mechanism. In these cases, voters should have to authenticate to a system before receiving the return identification information, such as by authenticating to their private e-mail accounts, or authenticating to the election jurisdiction's online ballot delivery system. Return identification information should be presented in a machine-readable format, and cryptographically integrity-protected using a secret key controlled by the election jurisdiction (e.g., a digital signature or cryptographic message authentication code).

### 4.2.4 Ballot Tracking

When state law or procedure mandates the use of ballot identifiers, these identifiers should be implemented in a manner that prevents linking the voter with his or her ballot choices. Systems storing ballot identifiers should protect this information from unauthorized disclosure through cryptographic and other technical means. For instance, ballot identifiers could be automatically generated by the system and stored in an encrypted format. Depending on legal or procedural requirements, the system should either not provide the capability to link a voter to a ballot, or the system should implement technical protections designed to protect this information from

unauthorized disclosure. There are a variety of cryptographic mechanisms that could be used to implement such features. If tracking information is printed on ballots, jurisdictions should consider printing this information in a form that is difficult to transcribe by hand, such as a barcode, as opposed to numbers or text.

As an alternative, tracking information can be written on ballot return envelopes or voter affidavits. Tracking information on these items do not pose ballot secrecy concerns, as they are detached from returned marked ballots before tallying.

In addition, marked ballots may be given tracking information during processing. For example, ballot privacy envelopes could be numbered after separation from the return identification information that identifies the voter. In this instance, care should be taken procedurally and technically so that the numbering of the privacy sleeves cannot be used in combination with other available information to link voters to ballots.

In most cases, jurisdictions receiving paper ballots that were printed by the voter will have to copy the voter's selections on the received ballot on to official ballot stock. In these cases, tracking information should be written to both the original ballot received from the voter, and the transcribed ballot on official ballot stock that links the two ballots. This linkage does not impact ballot secrecy, as the identity of the voter has already been separated from the completed ballot.

#### **4.2.5 Ballot Preparation**

The EAC's Election Management Guidelines [28] and the Ballot Preparation/Print and Pre-Election testing Quick Start Guide [30] provide some best practices that may help jurisdictions identify procedures for preparing ballots prior to an election.

Blank ballots that are intended to be e-mailed or posted on Web sites should be converted directly into a publically-available document format. For example, many jurisdictions use the Portable Document Format (PDF) [21]. Notably, due to file size considerations, ballots should not be merely scans of printed paper ballots.

Some publically-available document formats support electrically-fillable forms, which could be used to allow voters to make their choices on their computers, even though they are expected to print the ballot and sign accompanying forms. As noted in Section 3.2.4, many formats have extensions that support scripting languages that can be used to help voters avoid mistakes when filling out forms. For instance, Javascript can be used

in the PDF format to warn voters if they overvote. However, these extensions can cause compatibility problems and introduce a variety of potential security vulnerabilities. In particular, jurisdictions that decide to use these extensions should ensure the forms work even in document viewing applications that do not support those extensions, or have them disabled (e.g., Javascript may be disabled in many PDF readers for security reasons).

Some publically-available document formats, such as PDF, support digital signatures. Jurisdictions may consider digitally signing blank ballots prior to e-mailing or posting them in order to give voters additional assurance that they received the correct, unaltered forms. For these signatures to be effective, jurisdictions must obtain a digital certificate from a certificate authority that is trusted in widely-used document viewers. There are several commercial certificate authorities which sell certificates that can be used to sign documents, although these are less common than other types of certificates. State and local jurisdictions may also be able to use a certificate authority operated by the state, particularly if the state's certificate authority is affiliated with the federal government's certificate authority.

The benefits of signing documents should be weighed against the costs of obtaining the software and digital certificates necessary to support document signing. Most voters will not notice the difference between a signed document and an unsigned document, limiting the security benefit. For that reason, election officials may want to consult with other agencies in their jurisdiction to determine if another agency already has the requisite software and digital certificate to sign documents.

If an online ballot marking tool is being provided to voters (discussed further in Section 4.6), constructed ballot definition files should be produced and tested using the same procedures that jurisdictions use to produce and test ballot definition files for polling place systems. For instance, jurisdictions should implement technical and procedural controls to ensure the accuracy and integrity of the information on in the files. After loading the ballot definition files in the ballot marking tool system, election officials should test the system to ensure the proper candidate and ballot question information will be displayed to voters.

### **4.3 Fax Transmission**

Jurisdictions should follow their standard procedures for ensuring ballots are correct before faxing them to voters. Election workers faxing documents should remain near the fax machine as the ballot is sent to ensure no one disrupts the sending process or to deal with any errors that might arise.

Most fax machines keep a log of faxes that are sent and received. This includes successful and unsuccessful transmission. These logs may be useful auditing records to keep, but also could also allow voters' telephone numbers to be disclosed to unauthorized parties if fax machines are not kept in secure locations, since these logs are usually available to anyone with physical access to the machines.

As previously noted, some fax machines keep digital copies of sent or received faxes. While blank ballots and associated election materials (e.g., voter affidavits) typically will not include any sensitive information, some jurisdictions may wish to clear this information periodically.

#### **4.4 Electronic Mail**

Blank electronic ballots should be prepared as described in Section 4.2.5 to ensure the files have the best possible chance of being successfully delivered to voters, and contain the accurate candidate and ballot question information. Jurisdictions should follow their standard procedures for ensuring these blank ballots are correct before e-mailing them to voters.

Jurisdictions should beware of spam filters which may inadvertently mark their messages as spam and not display it to users. It is difficult to ensure that e-mails sent by jurisdictions will not be marked as spam. As previously noted, use of DomainKeys Identified Mail [10] on the jurisdiction's e-mail server may reduce the changes of outgoing e-mail being marked as spam. Jurisdictions may also consult the Message Anti-Abuse Working Group's *Sender Best Communications Practices* for additional technical measures [13].

E-mails should be addressed to voters individually, rather than sending a single e-mail to a group of voters. The "Reply-to" and "From" fields of the outgoing e-mail should be set to an e-mail account monitored by election officials. Election officials should closely monitor this e-mail account for any error messages that indicate a message was not properly received by the voter. Some types of e-mail error messages were described in Section 2.2.2.2. Election officials should read the error message to determine the nature of the problem and remedy it if possible, as it may be a sign of a technical malfunction. If the problem cannot be remedied, election officials should apply the same procedures used by the jurisdiction when it has evidence that a mailed ballot did not reach its destination.

## **4.5 Web-Based File Repositories**

Jurisdictions may post blank ballots on Web sites. This method offers security benefits over electronic mail, as there are widely deployed and used technologies (e.g., TLS) that can be used to protect the confidentiality and integrity of information in-transit.

Blank electronic ballots should be prepared as described in Section 4.2.5 to ensure the files contain the accurate candidate and ballot question information. Election officials should follow their standard procedures for ensuring these ballots are correct prior to loading them on the server. Access control mechanisms should be used on the server to protect the forms from unauthorized access or modification. The server operating system and Web server application should be configured and deployed according to widely accepted computer security best practices. For example, ballots should be delivered to voters using the HTTPS protocol using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

Voters will need to identify themselves to the system in order to allow the system to provide the correct ballot to each voter. As discussed in Section 4.2.1, voter authentication may or may not be necessary, depending on state law and local procedures. However, some form of authentication is required in circumstances where voters will receive return identification information that will be used as a secondary voter authentication mechanism when processing return ballots.

## **4.6 Online Ballot Markers**

Section 2.2.3.3 discussed various technologies for implementing Web-based applications for marking a ballot. Options such as Flash and Java require third-party plug-ins that, while widely deployed, are not present or enabled on all personal computers. DHTML, Javascript, and Ajax Web applications are supported in nearly all modern Web browsers, although these technologies are sometimes disabled for security reasons.

The Web server's operating system and election application should be configured and deployed according to widely accepted computer security best practices. Voters should interact with Web applications over an HTTPS connection using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites. The ballot marking tool is also a potential source for vulnerabilities in the system. The tool should be developed in accordance with widely

accepted best practices for Web application development, being careful to block common Web application vulnerabilities. NISTIR 7682 provides an overview of the security best practices for procuring, configuring and administering these systems.

The system will need access to voter lists that tell the system what ballot style should be delivered to each voter. In many cases, this information will be exported from the state or local jurisdiction's voter registration database and imported into the online ballot marking system. Maintaining the accuracy and availability of this data is critical, and jurisdictions should protect this information using similar technical and procedural controls to how they protect pollbooks and the voter registration database. If these voter lists contain sensitive information, possibly to facilitate voter identification or authentication, then it will also be important to protect the confidentiality of this information.

The system will need access to ballot definition files. These files should be produced and tested using the same procedures that jurisdictions use to produce and test ballot definition files for polling place systems. For instance, jurisdictions should implement technical and procedural controls to ensure the accuracy and integrity of the information on in the files. After loading the ballot definition files in the ballot marking tool system, election officials should test the system to ensure the proper candidate and ballot question information will be displayed to voters.

As with Web-based file repositories, voters must identify themselves to the system in order to allow the system to provide the correct ballot to each voter. As discussed in Section 4.2.1, voter authentication is not necessarily required, particularly if voters are not restricted from downloading their ballots multiple times. However, voters will need to be authenticated in circumstances where voters receive return identification information that will be used as an authentication mechanism when processing return ballots.

To protect ballot secrecy, the printable ballot should be constructed using software that runs solely on voters' computers. At no point should the ballot marking application transmit voter selections to the Web-server. However, Web applications may send information about the voter to the Web server, in order to supply proper candidate and ballot question information, and potentially to support return identification and ballot tracking mechanisms.

Printed ballots may contain machine-readable encodings of information on the ballot, such as ballot style, ballot ID, ballot questions and selections. Machine-readable encodings could take the form of barcodes, or text printed in a font compatible with optical character recognition. Any machine-

readable ballot information should also be available in human-readable form as well, except for information intended to protect the integrity of the machine-readable encoding (e.g., digital signatures, checksums, message authentication codes, or error correcting codes).

## 5 Other Resources

### EAC Election Management Resources

- Election Assistance Commission. *Election Management Guidelines*. [http://www.eac.gov/election\\_management\\_resources/election\\_management\\_guidelines.aspx](http://www.eac.gov/election_management_resources/election_management_guidelines.aspx)
- Election Assistance Commission. *Best Practices for Facilitating Voting by U.S. Citizens Covered by the Uniformed and Overseas Citizens Absentee Voting Act*. September 2004. [http://www.eac.gov/research/uocava\\_studies.aspx](http://www.eac.gov/research/uocava_studies.aspx)
- Election Assistance Commission. *Quick Start Guides*. [http://www.eac.gov/election\\_management\\_resources/quick\\_start\\_guides.aspx](http://www.eac.gov/election_management_resources/quick_start_guides.aspx)

Additional EAC election management resources can be found on the EAC Web site at <http://www.eac.gov>.

### NIST Computer Security Resources

#### **Guidelines**

- Draft NIST IR 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2010.
- NIST Special Publication 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. February 2010.
- NIST SP 800-60 Rev 1. *Guide for Mapping Types of Information and Information Systems to Security Categories* (2 Volumes). August 2008.
- NIST SP 800-53 Rev. 3. *Recommended Security Controls for Federal Information Systems and Organizations*. May 2010.
- FIPS 199. *Standards for Security Categorization of Federal Information and Information Systems*. February 2004.
- NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers, Version 2*, September 2007. <http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf>
- NIST Special Publication 800-123, *Guide to General Server Security*, July 2008. <http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf>



- Draft NIST Special Publication 800-63 Rev. 1, *Electronic Authentication Guideline*, December 2008.  
[http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1\\_Dec2008.pdf](http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf)
- NIST Special Publication 800-45, *Guidelines on Electronic Mail Security, Version 2, February 2007*.  
<http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf>
- NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.  
<http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>

### **Other NIST Resources**

- National Checklist Program (NCP). <http://checklists.nist.gov/>
- National Vulnerability Database (NVD).
- Security Content Automation Protocol (SCAP) Specifications.  
<http://scap.nist.gov/>

A wide range of additional computer security resources are available on the NIST Computer Security Resource Center Webpage at .

### **Federal Voting Assistance Program (FVAP) Resources**

- FVAP. *United States Postal Service Mail Guidelines*.  
<http://fvap.gov/leo/usps-mail-guidelines.html>
- FVAP. *Fax & E-mail Guidelines*.
- FVAP. *Guidelines for the Help America Vote Act*.  
<http://fvap.gov/leo/hava-guidelines.html>

The Federal Voting Assistance Program has set up a portal for election officials to obtain UOCAVA voting-related information and resources at <http://fvap.gov/leo/index.html>.

## 6 References

- [1] National Institute of Standards and Technology Interagency Report 7551, *A Threat Analysis on UOCAVA Voting Systems*, December 2008. <http://vote.nist.gov>
- [2] Draft National Institute of Standards and Technology Interagency Report 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2011. <http://vote.nist.gov>
- [3] EAC. (2010). UOCAVA Pilot Program Testing Requirements, March 24, 2010. Accessed May 10, 2010 at <http://www.eac.gov/program-areas/voting-systems/docs/requirements-03-24-10-uocava-pilot-program>
- [4] FVAP. (2010). Federal Post Card Application. Accessed May 10, 2010 at <http://www.fvap.gov/resources/media/fpca.pdf>
- [5] Testimony of Bob Carey, Director of FVAP. (2010) EAC Public Meeting, Dec. 3 2009. Accessed April 5, 2010 at [http://www.eac.gov/public\\_meeting\\_12032010/](http://www.eac.gov/public_meeting_12032010/)
- [6] National Institute of Standards and Technology Interagency Report 7770. *Security Considerations for Remote Electronic UOCAVA Voting*. Whitepaper for the Technical Guidelines Development Committee. February 2011.
- [7] Internet Engineering Task Force. (2010). S/MIME Mail Security. Accessed April 3, 2011 at <http://www.ietf.org/wg/concluded/smime.html>
- [8] Callas, J., Donnerhackle, L., Finney, H. and R. Thayer, "OpenPGP Message Format", RFC 2240, November 1998.
- [9] NIST SP 800-45 Version 2. Guidelines on Electronic Mail Security, February 2007
- [10] Hansen, T., et. al., "DomainKeys Identified Mail (DKIM) Development, Deployment, and Operations", RFC 5863, May 2010.
- [11] Sender Policy Framework (2010). Project Overview. Accessed June 18, 2010 at <http://www.openspf.org/>

- [12] Lyon, J., and M. Wong, "Sender ID: Authenticating E-mail", RFC 4406, April 2006.
- [13] Messaging Anti-Abuse Working Group. (2010). MAAWG Sender Best Communications Practices Version 2.0. Accessed June 18, 2010 at
- [14] Dierks, T., and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.
- [15] NIST SP 800-60 Rev 1. Guide for Mapping Types of Information and Information Systems to Security Categories (2 Volume). August 2008.
- [16] NIST SP 800-53 Rev. 3. Recommended Security Controls for Federal Information Systems and Organizations. May 2010.
- [17] Draft NIST SP 800-128. Guide for Security Management of Information Systems. March 2010.
- [18] Draft NIST SP 800-34 Rev. 1. Contingency Planning Guide for Federal Information Systems. October 2009.
- [19] FIPS 199. Standards for Security Categorization of Federal Information and Information Systems. February 2004.
- [20] "Uniformed and Overseas Citizens Absentee Voting Act", P.L. 99-410
- [21] ISO 32000-1:2008, Portable Document Format—Part 1: PDF 1.7.
- [22] Microsoft. (2010). Microsoft Office File Format Documents. Accessed May 10, 2010 at <http://msdn.microsoft.com/en-us/library/cc313105.aspx>
- [23] Accessibility and Usability Considerations of Remote Voting Systems. Whitepaper for the Technical Guidelines Development Committee. <http://vote.nist.gov>
- [24] GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008.
- [25] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010.

- [26] Federal Trade Commission. (2008). FTC Consumer Alert: FTC Cautions Consumers About Voter Registration Scams. Accessed May 10, 2010 at
- [27] Committee on State Voter Registration Databases; National Research Council. (2010). Improving State Voter Registration Databases. Accessed June 3, 2010 at
- [28] Election Assistance Commission. (2010). Election Management Best Practices. Accessed June 18, 2010 at
- [29] Election Assistance Commission. (2004). Best Practices for Facilitating Voting by U.S. Citizens Covered by the Uniformed and Overseas Citizens Absentee Voting Act. Accessed June 18, 2010 at
- [30] Election Assistance Commission. (2006). Quick Start Guide: Ballot Preparation/Printing and Pre-Election Testing. Accessed Jun 18, 2010 at

## **Appendix A: General Computer Security Best Practices**

A variety of system components will play a role in transmitting election materials electronically. Some of these components will likely serve multiple functions within a jurisdiction, and most are likely to be managed by technical personnel who also maintain information technology (IT) systems which are unrelated to the transmission of election materials. Close coordination will be required between election officials and technical personnel to ensure that sufficient process and technical controls are in place for the secure deployment of such a system.

Security requirements for systems that contain election materials will differ according to local regulations and practices as well as according to the nature of the materials contained on the system. Even so, certain basic practices need to be followed to secure any important IT system.

This section outlines those general best practices and will help election officials understand the points of coordination required for a secure, functional system. Once the security objectives are identified as part of the system characterization process, a set of security controls will be established to meet these objectives. Some of the controls will be common to many or all systems within the organization, and some may be specifically deployed in support of the election system.

### **A.1 System Characterization**

The first step in securing any system is the establishment of security objectives. In order to select appropriate security measures, election and IT personnel need to have a common understanding of the confidentiality, integrity and availability requirements for the system's data and functions. This requires a thorough description of the system's purpose, data, components and boundaries.

Election officials should work with technical staff to identify or create documentation of the purpose and scope of every system. The resulting characterization will drive planning for fulfilling the system's security objectives. For example, a system whose purpose is delivering information on application deadlines may contain only public domain information that is readily available through other channels, and therefore would not have any confidentiality requirements, might have moderate integrity requirements, and low availability requirements. A system that allows voters to view and modify their registration information might introduce moderate or high confidentiality requirements, depending on the sensitivity of the information displayed.

### **A.1.1 Functional Description**

As a first step to characterizing the system, each function provided by the system must be defined along with who will access that function. In most cases, any technical details expressed in the functional description should be very high-level. For example, election officials may be able to load ballot configuration files on a system, or voters may be able to update their voter registration information on the system. For each function provided by the system, assess the risk posed by failure to provide it. In assessing this risk, it is important to consider legal and procedural requirements unique to the jurisdiction, as these will influence and may even explicitly define the impact of unavailability for some election-related functions.

### **A.1.2 Data Categorization**

In order to provide the functions documented in the functional description, the system will require access to various types of data. Determine what data must be stored on or processed by the system in order to provide each function. Here also, any technical details expressed in the data characterization will be very high-level. Each type of data should be described according to confidentiality, integrity, and availability requirements. For each, establish the impact of improper disclosure, modification or destruction of that data. As with availability of system functions, each jurisdiction may have specific circumstances or legal requirements that help determine this impact. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* [15] details preliminary characterizations for certain types of data, which may provide a useful starting point. For all other data, this document provides readers with a list of common considerations to use when determining impact levels.

As a general best practice, systems should not store or access any data beyond that which is required to provide an election function identified in the functional description if that data has any confidentiality or integrity requirements.

### **A.1.3 System Architecture**

The description of the system architecture will contain more granular technical details than either the functional description or the data categorization. Election officials should work with IT personnel to describe the components (e.g., servers, routers, workstations) that will be used to deliver the system functions previously enumerated. It is important to understand the role of each component in delivering the system's functions along with what data will be stored in or processed by each. The system

architecture description should account for how component failures could compromise availability, confidentiality or integrity.

All physical and logical boundaries should be established in the system architecture. These should include both technical and organizational considerations. So, for example, any common resources shared across boundaries (e.g., network storage used for both election and other county data) should be identified so that sufficient technical and procedural controls can later be defined.

## **A.2 Identification of Common Controls**

The IT system deployed to support the transmission of election materials will most likely be one of many systems managed by the jurisdiction. In this case, the organization responsible for the operation of the IT systems will have established certain common security controls that apply to all systems and hosting facilities controlled by that organization. These controls should be analyzed in conjunction with the security requirements established during the system characterization for the election system. Election officials should work with the IT management organization to understand which common security controls exist. Together, they should identify both how these common controls can be used to support the voting system security requirements and where new controls need to be deployed along with the new system.

Because system management services will most likely be shared with non-election systems, certain management policies will most likely be common across the organization. Several of these are relevant to system security and merit specific consideration in the context of a system used to process election data:

- Personnel screening is the process by which the organization determines that individuals are suitable for performing specific duties. Election officials should ensure that this process complies with any relevant regulatory requirements governing personnel with access to the types of data identified in the data characterization.
- Configuration Management is the set of policies and processes for controlling system and documentation modifications. Related controls are discussed in detail appendix A.4.
- Contingency Planning is the set of policies and processes intended to maintain and restore election operations in the event of emergencies, failures or disasters. Related controls are discussed in further detail in appendix A.5.

- Physical Access Controls are policies and procedures that govern how personnel gain physical access to systems and facilities. For some components of the system, physical access may imply access to election data which should be identified in the system architecture. Election officials should confirm that the organization's physical access controls on such components are sufficient to meet local requirements.
- User Identification and Authentication controls govern how the system determines a user's identity. The technical details of using these controls to verify identity claims are discussed in NISTIR 7682 [2] and are outside the scope of this document. Election officials should examine the process the organization uses to issue the credentials used for user identification for those users who might have access to sensitive system data and confirm that this process meets applicable regulatory requirements.
- Hardware and Software Acquisition channels are likely to be shared across the organization. Election officials should confirm that this process meets any election-specific requirements.
- Incident Response Procedures are intended to detect, respond to, and limit consequences of IT security compromises. These are discussed in greater detail in appendix A.6.

Certain technical controls are also frequently applicable on a facility-wide basis and therefore tend to be shared by many unrelated systems. These include:

- Physical/environmental aspects of the facility such as availability monitoring, backup power supplies, fire suppression, and media storage.
- Local and remote network access for jurisdiction personnel.
- Network Infrastructure Protections, such as those described in the Appendix B.

In addition to common security controls, many jurisdictions will use existing network infrastructure to service some of the functional requirements for the election system. For example, some systems existing as DNS servers, e-mail servers or Web servers will likely be used. Just as with components specific to the election system, the architecture description developed during the system characterization should identify functions provided by and data processed by or stored on the shared components. For this shared infrastructure, election officials should coordinate with those systems' managers to ensure that the system-specific controls are sufficient to meet the security objectives defined for those functions and data.



### **A.3 Network and Communications Protections**

Even with effective security controls configured for those hosts which provide election-related functionality, certain network and communications infrastructure protections need to be in place to support the secure operation of the overall system. In many cases, the network infrastructure owned by a jurisdiction may be used to support both election and non-election functions. The system architecture description developed during the system characterization should identify security objectives for the shared components. Election officials should work with IT management to examine the protections in place on these shared components and ensure that they are adequate to provide the required availability, confidentiality and integrity guarantees for the election system.

Appendix B provides a more detailed discussion of proper network and communication protections that are appropriate for use with a voter registration, ballot request, or blank ballot delivery system.

### **A.4 Configuration Management**

Any IT system that provides a mission-critical function for an organization should have a formal, documented set of policies and procedures for security configuration management. In many cases, the policies will not be system-specific, but will be organization-wide. Existing policies and procedures should be examined and assessed to determine whether they are adequate for meeting the security objectives of the election system or whether system-specific augmentations are required. Whether or not the policies and procedures need to be changed, election officials need to be identified as stakeholders in the configuration management process and play an active role in planning and validating configuration changes.

NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* [16], details Configuration Management controls that may be appropriate to differing levels of security objectives, and NIST SP 800-128, *Guide for Security Configuration Management of Information Systems* [17], describes how specific parts of the configuration management process support these controls.

#### **A.4.1 Configuration Management Planning**

Election officials should review the plan for managing the security configurations of systems that will be used to support the transmission of election materials. Although the IT management organization will generally own the plan, as stakeholders, election officials should review the plan at a high level to ensure that it includes:

- Well-defined roles and responsibilities for personnel involved in proposing, testing, approving and implementing configuration changes
- A description of how configuration items are selected for management control
- A process for establishing a secure baseline configuration
- A process for managing updates to the baseline configuration

In many cases, if an organization has a mature, formal configuration management plan in place, the only augmentation required will be the addition of election officials to key planning, approval and testing roles.

#### **A.4.2 Secure Baseline Configurations**

A secure baseline configuration is a documented set of specifications for a system or component that has been reviewed and agreed upon by the stakeholders of a system. The secure baseline configuration can only be updated by following the process outlined in the secure configuration management plan, and should always reflect the state of the current system.

IT organizations are likely to have secure baselines that apply to many components of a particular type (e.g. file servers). These configurations may then need to be supplemented to meet the security requirements established during the system characterization. The system architecture description should identify each component of the system along with the functions it provides and data it stores or processes. Election officials should work with technical personnel to review each component against the standard secure baseline configuration and determine whether the security objectives are met by the baseline, or to develop a new baseline specific for the election system.

All configurable components which play a role in maintaining the security or availability of the system should have secure baseline configurations.

#### **A.4.3 Change Control**

Change control is the documented process by which configuration changes are proposed, justified, implemented, tested and reviewed. Every organization needs to have a change control process which applies to all components involved in the transmission of election materials. This should include changes made to hardware, software, operating systems and applications. Election officials need to ensure that they are involved in the testing and approval of changes that could impact the security or availability of these systems.

Jurisdiction-specific regulatory and procedural requirements may influence the level of scrutiny and approval required for system changes. Election

officials should verify that the change control process meets their jurisdiction requirements.

## **A.5 Contingency Planning**

Contingency planning refers to the collection of plans, procedures and technical measures which will be used to ensure continued availability of system functions in the event of potentially disruptive events. This covers a broad scope of planning activities aimed at ensuring resiliency of system functionality. Election officials should work with technical staff to ensure a solid mutual understanding of system availability requirements and gain assurance that adequate contingency plans are in place.

In most cases, contingency planning activities will cover all critical systems managed by an IT organization and hosted in a particular facility. Election officials should consult with technical staff to ensure that the plans in place are commensurate with the availability requirements described in the system characterization documentation, and that these plans do not compromise the confidentiality or integrity requirements established for the data. So, for example, if local requirements state that access to voter records must be logged, officials should ensure that access to off-site backups containing voter records is similarly logged. NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems* [18], gives examples of contingency planning strategies that map to the impact levels described in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* [19].

### **A.5.1 Preventative Controls**

Preventative controls are established in advance of an event and are aimed at preventing that event from causing a disruption to system functionality. Examples of these controls include short-term, and possibly long-term, backup power supplies, duplicate or backup communication lines, fire suppression systems and regular preventive maintenance. These preventive controls should be commensurate with system availability requirements. In most cases, the fact that a system transmits election data will not impart special requirements for preventive controls in a facility that houses other mission-critical systems.

### **A.5.2 Backup and Recovery Strategies**

Backup and recovery strategies cover those plans and procedures used to restore system operations following a service disruption. Election officials need to understand the allowable downtime for their application and work with technical staff to develop a backup and recovery plan which can restore service without exceeding that threshold. One practice common to all backup

approaches is storage of backup data at a location distinct from the live system.

Backup and recovery strategies need to address outages caused by events from a variety of failures, from simple equipment failure to major natural disasters. Recovery strategies from major long-term failures will rarely be system-specific. For more localized disruptions, there is a substantial advantage to using standard hardware across the IT organization where possible and ensuring that enough spare equipment is available to quickly replace the system and restore the software and data on the system using the backup media. In addition to standardizing equipment and verifying the availability of spares, election officials should ensure that backup hardware is acquired for any election system-specific equipment that could cause an outage to exceed the availability requirements in the event of a failure.

### **A.5.3 Plan Testing**

Contingency plans need to be tested according to availability requirements established when characterizing the system. The goal of testing is to ensure the availability targets are maintained. Election staff should work with IT staff to participate in the tests. This provides the opportunity to confirm that all roles and responsibilities are identified and well understood, prior to an actual disaster. The organization's contingency plan should provide for regularly scheduled testing and should define events that trigger a new test exercise (e.g. turnover of key personnel, facility change, etc.).

## **A.6 Incident Response**

Jurisdictions should ensure that a computer security incident response plan is in place prior to system deployment. Both election officials and IT personnel will have key roles in the incident process.

The incident response plan should clearly define which systems are covered and what constitutes a security incident for each one. Any system involved in the transmission of election data should be covered by an incident response plan. There should be a process for defining an incident's severity and establishing the priority for responding to that incident. Jurisdiction officials should have input into the criteria for severity and priority.

Roles, responsibilities and authority should be clearly documented for various classes of security incidents. Individuals should be identified, and the plan should include details of on- and off-hours communications channels to be used according to incident severity and priority. The plan should also establish a process for approving discontinuation of service in the event of an ongoing incident. Both IT and election representatives will need to be

involved in this process. In most incident response plans, because the initial response will focus on halting an active incident and preserving evidence for later analysis, the initial response will primarily be handled by the technical staff charged with operating and monitoring systems. After the incident, election representatives are likely to have a more central role, as decisions will need to be made on technical or procedural changes to the system as service is restored. Election officials will need to be familiar with any local, state or federal requirements governing notification of affected individuals in the event of a data breach.

Election officials should ensure that the incident response plan addresses any specific legal issues that arise from the nature of the system. For example, some states have specific disclosure procedures that need to be followed in the event of compromise of Personally Identifiable Information.

As with contingency plans, incident response plans should be tested prior to system deployment and periodically thereafter.

### **A.7 *Continuous Monitoring***

All security controls should be assessed prior to system deployment. For critical systems, a subset of management, operational and technical security controls should be continuously monitored in several ways, all with the goal of ensuring that system security and availability objectives are met on an ongoing basis as operations continue. Many IT organizations may include continuous monitoring provisions in various plans and policies rather than consolidating these activities under one plan.

Automated network and system monitoring tools should be used and monitored to detect integrity or confidentiality breaches. These tools may monitor log files, network traffic, file changes, etc. IT organizations should have a documented process for responding to output from these tools.

Network and host configurations should be periodically inspected and assessed to ensure they are compliant with current secure baseline configurations. This should involve both automated testing using some combination Security Content Automation Protocol (SCAP)-based tools and the automated system monitoring tools for other purposes and periodic audits. In particular, election officials should ensure an individual is identified and tasked with reconciling log entries which identify security-relevant system configuration changes with configuration management records. This is intended to ensure no change is made to the system without following the required testing and approval process established in the configuration management plans. IT staff should identify which configuration settings can

be automatically monitored and which require manual action by the auditor to inspect the settings and confirm that they match the most recent configuration management records for the deployed system.

Election officials should verify that the IT department identifies an individual or a team tasked with monitoring for public reports of vulnerabilities in the components that comprise the system, as well as common components that serve to support the system. This enables the organization to respond to potential vulnerabilities even in the interval between public disclosure and vendor response.

The continuous monitoring plan should provide for periodic security testing. Some tests can be conducted using only automated tools, which is both inexpensive and beneficial to all the systems managed by the jurisdiction, not solely those used to support elections. Other security tests require specialist expertise which is both quite costly and frequently system-specific. Election officials should work with the IT organization to prioritize and schedule tests according to the impact of a potential security breach on the system.

If any of these mechanisms detects an exception, the monitoring plan should include a process for assessing whether or not the exception is also a security incident. If it meets that definition, the incident response plan should be invoked. Otherwise, there should be a flaw remediation plan in place for reporting and addressing the issue, and updating the secure baseline configuration if necessary.

The continuous monitoring process should be periodically tested, to ensure that exceptions are properly flagged and remedied by the organization.

## **Appendix B: Component Security Considerations**

This appendix offers security considerations for specific components likely to be used in the delivery of election materials to voters, such as network infrastructure, Web servers, e-mail servers and e-mail clients. This is not intended to be a comprehensive guide to all security considerations inherent in configuring such components. Rather, it seeks to reference other materials and identify considerations that are likely to pertain to these system components when they're used to transmit election materials and to guide election officials in collaborating with technical staff to ensure that components are configured and operated in a manner consistent with the security objectives of the system.

This appendix is directed toward readers with a high-level technical understanding of the components used to deliver the business functions of the system. It should assist such a reader in interacting with the technical personnel charged with implementing and managing the system. Prior to considering the guidance in this appendix, the reader should understand the System Characterization and the resulting security objectives.

The information in this appendix is intended to supplement, not replace, the best practices in NISTIR 7682. The security practices discussed in that document are critical for all of the systems discussed here. This information is intended only to help the reader better understand the application of those practices for this purpose.

Decisions about which technical controls and protections apply to various system components are driven by the system characterization. Some of these protections will be common, applied to every system the IT organization operates. Others may be specific to components of systems used to deliver election materials. Election officials and technical staff will need to identify areas where existing controls may need to be augmented in order to comply with relevant federal, state and local regulations for protection of the information stored on or accessible via these systems.

The system characterization will have defined the components necessary to fulfill its intended functions. In general, secure deployment of these systems implies that they do exactly what's specified in the characterization and no more. This means that the systems should only store the minimum amount of data necessary to perform their function, only be connected to those other systems required by the characterization, and only be accessible by those individuals who are authorized to have access.

## ***B.1 Network Infrastructure Protections***

### **B.1.1 Establishing Security Boundaries**

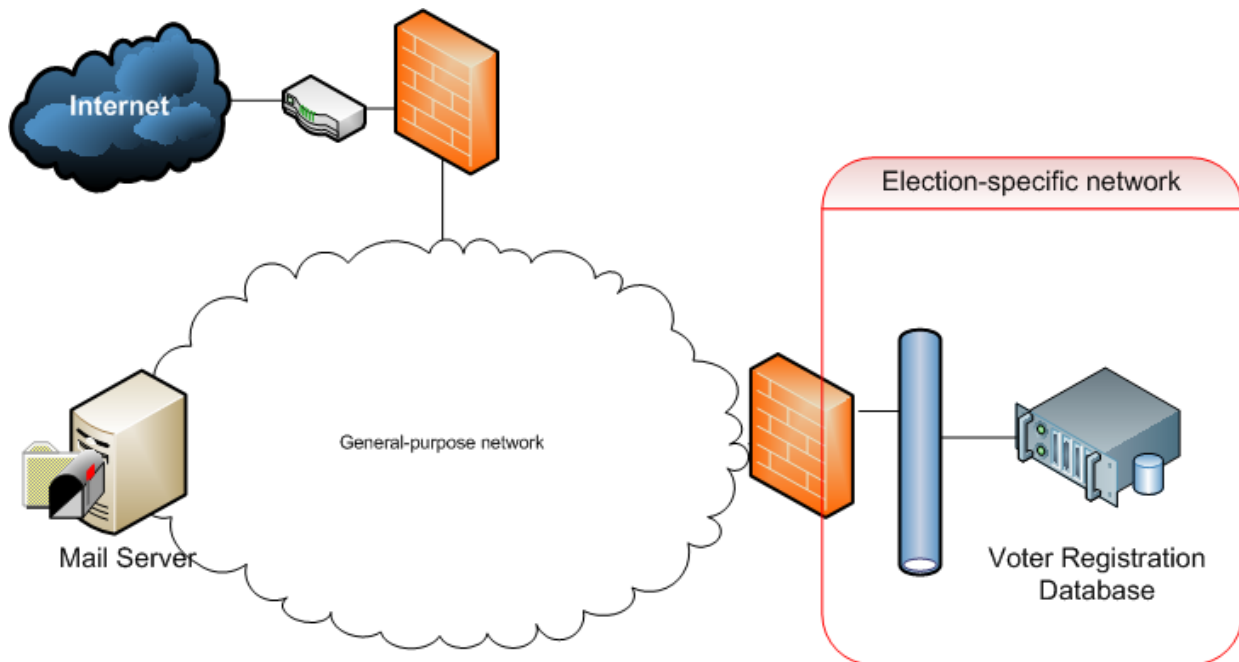
The system architecture and security objectives produced during the system characterization can then be used to identify specific network infrastructure components and their roles in protecting the system. These components (routers, switches, hubs, firewalls, etc.) can then be classified. Election officials should work with technical staff to identify the security controls which are active for these components, and confirm that these are sufficient to maintain the system's overall security objectives. This enables the establishment of boundaries to control the flow of sensitive information.

The system architecture should be analyzed with an eye toward information flow. Each information object that traverses a piece of network infrastructure should be identified along with the security requirements for that information and the security controls in place for that infrastructure. Information should only traverse network infrastructure with controls sufficient to protect it. If information needs to be sent through infrastructure without sufficient controls to protect it (for example, PII needs to be sent across an organization's general business network) additional measures, such as encryption should be identified and put into place. Threats to information and measures which address those threats are identified in detail in section 4 of NISTIR 7682. Technical protections for network infrastructure are addressed in section 5 of NISTIR 7682.

Components with differing security requirements should be connected to physically distinct networks when feasible. For example, a jurisdiction's Web server and voter registration database will generally have incompatible confidentiality requirements. Ideally, these should not be connected to the same network infrastructure. In many cases such an "air gap" will be impractical or even impossible, due to business considerations. In such cases, additional network protections such as firewalls and application proxies should be used to enforce logical separation at these boundaries.

The business and technical teams need to collaborate to devise rules for exactly what information should be allowed across these boundaries and configure the network protections accordingly. So, for example, two unrelated systems that need to be colocated for budgetary reasons but have no need to share data with each other might be placed onto separate Virtual LANs (VLANs) using a managed network switch. A public server that needs access to portions of a protected database of record might be granted limited access to that database using firewall rules and a back-end application server.





**Figure 1. Segmenting election-specific infrastructure from the general-purpose network**

### **B.1.2 Considerations for Shared Infrastructure**

In most cases, some components of the system for transmitting election information will support multiple systems. The security-relevant functionality of these shared infrastructure components should be identified. The jurisdiction and the IT organization should work together to understand the security controls that are in place for the existing infrastructure, and evaluate whether these match the security requirements for the election system. For example, on most systems, a compromised or incorrectly configured DNS server, switch or router could cause e-mailed ballots to be improperly delivered, or grant an attacker the ability to alter them in transit. In such a case, security controls on these shared components should be analyzed against the security objectives of ballot delivery. Election officials should verify that the controls on security-critical shared components meet the security objectives identified for all election-specific functionality that depends on these components. So, in the example above, configuration controls need to meet the security objectives identified for e-mail availability and integrity.

Components that are likely to be shared include Web servers, e-mail servers, DNS servers, workstations, switches, firewalls and routers. Web servers and e-mail servers are discussed in more detail in later sections of this appendix as well as in NISTIR 7682 and in Special Publications 800-44

and 800-45, respectively. Workstations are discussed in the context of e-mail clients later in this appendix and more generally in NISTIR 7682. For detailed guidance on DNS security, see SP 800-81. Best practices for securing all of these infrastructure components are covered in NISTIR 7682.

Both election and IT stakeholders should ensure that common controls discussed in section 3.2 are considered for all shared infrastructure.

In cases where it is impractical to apply protections required by the sensitivity of the election system to the general-purpose infrastructure, jurisdictions should consider deploying dedicated infrastructure components in support of the election application.

## **B.2 E-mail Server Security**

As part of the system characterization, application owners should identify the role of e-mail in transmitting election information. Specifically:

- What kind of election information will be transmitted outside the organization via e-mail?
- What election information will be received from the public via e-mail?
- What election information might be stored (generally temporarily) on an e-mail server?

### **B.2.1 Outbound E-mail Security**

In most cases, the transmission of election information will bring no unique security requirements for outgoing e-mail. The best practices described in SP800-45 will all apply to the server that process outbound e-mail.

Because the public will consider e-mail originating from election officials to be trusted, care should be taken to verify that only authorized entities can use the organization's outgoing e-mail server to send messages, and that all outgoing messages are scanned for malware.

In order to increase the likelihood that election information will be correctly delivered via e-mail and increase the likelihood that forgeries from external parties will be flagged as such, jurisdictions should configure forgery countermeasures such as Domain Keys Identified Mail (DKIM) on servers that send election materials via e-mail. While not all voters' mail providers will recognize such protections, delivery reliability will be significantly improved when communicating with those providers that do process the additional verification data.

Organizations should ensure that all outbound e-mail connections require authentication with at least a user name and password.

Organizations should avoid transmitting information via e-mail if it's considered sensitive to disclosure according to local, state or federal regulations.

The outbound e-mail server should return any error notifications it receives to the sender of the e-mail for further analysis. Most servers will do this by default.

System owners should confirm that the maintenance process specifically ensures that malware signatures are kept current.

### **B.2.2 Inbound E-mail Security**

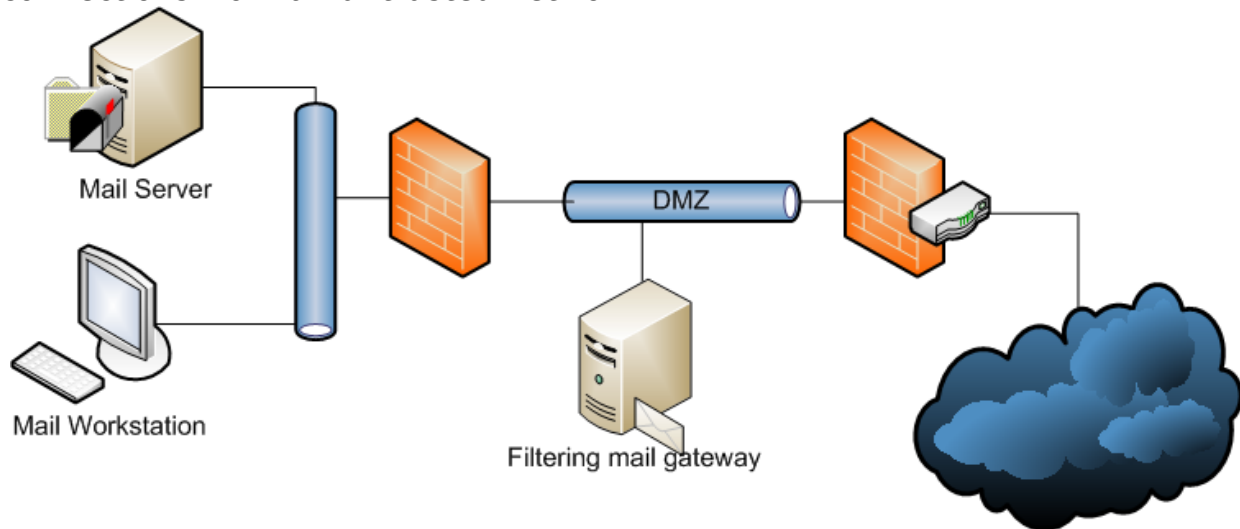
In applications where election officials receive completed forms from voters, additional specific considerations may be relevant. In particular, users of the mail server will need to open attachments received from the public over the Internet in order to perform their job functions. This increases the organization's exposure to malware. Additionally, such completed forms are likely to be stored on a mail server at least until they have been processed. This storage may introduce specific requirements, depending on local, state or federal regulations.

Election officials should work with the IT organization to ensure that access to the mail server is sufficiently controlled to meet these requirements. It may make sense for officials who receive such information to have mailboxes located on a server dedicated to election information.

Whether or not such a dedicated server is necessary, these considerations suggest that an architecture which incorporates an incoming mail gateway is preferred when e-mail is used for inbound election materials.

Incoming SMTP connections from the Internet should be routed through the mail gateway. The mail gateway should scan message content and filter or quarantine suspicious messages prior to delivering them to the internal mail server. If possible, this gateway should be configured to verify that attachments are of the expected type and fall into the expected size range, in addition to checking for malware. These gateways should also be configured to verify DKIM signatures on inbound messages. Ideally, the internal mail server should scan the message content a second time, using anti-malware software from a different source than the mail gateway. This architecture serves to reduce potential exposure to malware as well as to

ensure that messages are not stored on a machine which accepts connections from an untrusted network.



**Figure 2. Common architecture for incoming e-mail**

System owners should confirm that the maintenance process specifically ensures that malware signatures are kept up-to-date.

SP 800-45 details additional security best practices for e-mail servers.

### ***B.3 E-mail Client Security***

As with other components, information categorized as part of the system characterization will determine specific e-mail client security concerns. The best practices documented in NISTIR 7682 for workstation security and in SP 800-45 for e-mail client security will apply to all clients. Because e-mail clients need to interact with untrusted data, these security practices are particularly important. Care should be taken to ensure that configuration management practices are actively maintained, especially with regard to patching the OS and applications and maintaining the currency of malware signatures. Those workstations which receive completed forms as attachments, sent by the general public over the Internet, merit additional considerations.

First, it's almost inevitable that a workstation used to retrieve such e-mail will store voter information, even if only temporarily. Election officials should verify that the workstation meets any specific local, state or federal requirements for systems used to store such information.

Additionally, since such attachments may be constantly solicited (and therefore will always be expected by the workstation operator) and are received through an untrusted channel, the risk of malware infection is elevated. To counter this risk, election officials and administrators should verify that up-to-date, active malware protection is installed on the system. It is further beneficial if this protection uses signatures from a different source than the protection installed on the mail server.

As with all e-mail clients, active features like scripting support, automatic opening of e-mail and e-mail previews should be disabled. When attachments are used, system owners should pay similar attention to disable these features in any software used to process these. So, for example, in Microsoft Word, macros should be disabled. In PDF processing software, javascript, ActiveX and the execution of external applications should be disabled. Future versions of PDF-processing software continue to incorporate additional security features. As part of the continuous monitoring process, an individual should be identified to monitor new releases of any software used to process attachments and fast-track versions with new security features into production.

To further mitigate the threat of malware, it is a good practice to use a dedicated machine for monitoring a mailbox that actively solicits messages from the general public. Sensitive data and critical applications should be kept to a minimum on this workstation, and it should not be used for other important election functions.

As with all applications, proper user training is a key factor in the security of the system. In this case, the users who retrieve and read these attachments should be trained to recognize the expected type and size of attachment and seek assistance prior to opening any that fall outside these parameters.

#### ***B.4 Web Server Security***

Security considerations for Web servers will vary greatly depending on the role the server plays in delivering election information. For most systems, the Web server's role in the system will be broadly characterized in one or more of the following ways:

- Delivers non-personalized election information to the public
- Delivers personalized election information to the public
- Receives information from the public.

Certain common security practices for Web servers will apply to a server in any of these roles, including:

- Minimize software installed on the Web server
- Keep server software up-to-date
- Validate all user-supplied input
- Minimize the use of active content
- Restrict the privilege of the server process
- Separate the privileged administrator interface for managing the Web application from the unprivileged user interface.

Detailed guidelines for securing public Web servers can be found in SP 800-44. Additional general guidelines for Web application security are summarized in section 5.10 of NISTIR 7682. This section will not generally aim to repeat those, but will focus on specific concerns relative to the above functions.

#### **B.4.1 Encryption**

Because members of the public will consider the jurisdiction a trustworthy source of information, all Web servers supplying the public with election information should use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to provide authentication of the server's identity even in cases where the information being served is not sensitive. Domain-verified TLS server certificates are available inexpensively or without cost, depending on the vendor, and will assure voters that information was not modified in transit.

Organizations should ensure that Web servers are configured to allow only NIST-approved SSL/TLS configurations. Specifically, only SSL 3.0 or later and TLS 1.0 or later should be used, and the cipher suites should be restricted to those identified in section 4 of NIST special publication 800-57 (part 3). Key sizes should be selected using the guidance in section 2 of the same special publication.

#### **B.4.2 Delivery of Non-Personalized Information**

In most cases, servers containing only non-personalized election information will not have additional specific technical concerns. Election officials should verify that proper procedures are followed for publishing this information so as to comply with relevant local, state and federal regulations. Information owners should work with IT staff to use technical controls that enforce these procedures.

#### **B.4.3 Delivery of Personalized Information**

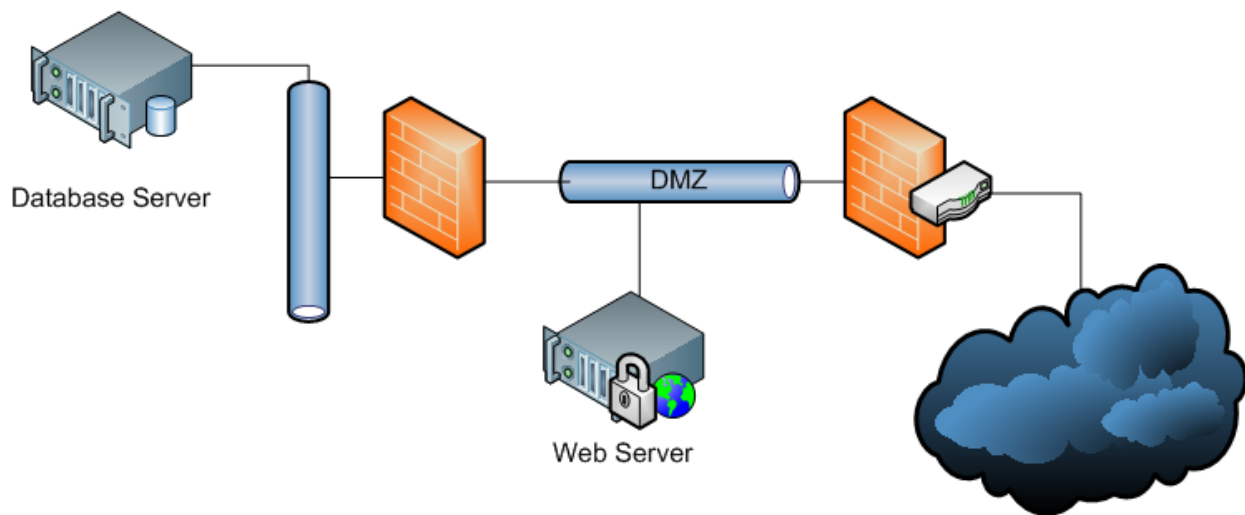
Servers that deliver personalized information to the public may require access to information deemed sensitive. In this case, some verification that information is only being delivered to the correct individual will be required.

Election officials should ensure that this verification meets applicable regulations.

If the personalized information being supplied to the voter is not public, measures should be taken to prevent automated processes from attempting to brute-force this verification process. Such measures might include:

- Challenge-response tests such as CAPTCHA which require human intervention before a server will process a request
- Limitations on the number of times a specific voter's information may be queried within a pre-determined timeframe
- Requiring the user to supply a pre-shared response sent through another channel, e.g. to a voter's previously registered e-mail address, postal address or phone

If the Web server requires access to sensitive information, the repository (usually a database) containing this should be stored on a protected network which is not directly accessible from the Internet. An example of such an architecture is in found in the figure below.



**Figure 3. Common network architecture for an Internet-accessible Web server**

Care should be taken to ensure that access by jurisdiction officials to any sensitive information stored in the database also complies with any relevant regulations.

#### **B.4.4 Receipt of Information**

Web servers used to receive information from the public have three unique security considerations which may vary depending on the type of information transmitted.

- Confidentiality of submitted information – If voters are submitting sensitive information to the jurisdiction using the Web server, controls must be established to prevent this data from being improperly disclosed.
- Protection of jurisdiction systems – Submitted information must be properly validated to guard against introduction of malicious content onto the jurisdiction’s protected network.
- Protection of other external system users – Information submitted by one untrusted user should not be viewable by other users.

The common security practices described in SP 800-44 and NISTIR 7682 aimed at protecting confidentiality and preventing active injection attacks (SQL injection, cross-site scripting, CSRF, etc.) all serve to address these considerations.

One common case that is of particular concern interest in the context of election systems is the submission of files for processing by election officials, especially PDF forms. When a user uploads a file, it should be quarantined in a location that is not readable by the Web server. This could be a filesystem directory to which the Web server context only has write access, a “drop box” on another server, or even a form which is submitted to a dedicated upload server. As with files received via e-mail, these files should be scanned for malware prior to processing by election officials.

Ideally, as with e-mail clients, initial processing of these files would occur on a workstation dedicated to this purpose. If possible, these files should be scanned for malware both at the time they are stored and at the time they are retrieved, preferably by different scanning engines. The same precautions outlined for e-mail clients should be followed when processing received files that may contain active content.

In addition to ensuring that these files cannot be served to other Web users, officials should work with technical staff to establish controls on the file repository which limit internal access to duly authorized personnel.



## Appendix C: Glossary

Access Control	The process of granting or denying specific requests for obtaining and using information and related information processing services.
Certificate	Also known as a digital certificate. A digital representation of information which at least <ol style="list-style-type: none"> <li>1. identifies the certification authority issuing it,</li> <li>2. names or identifies its subscriber,</li> <li>3. contains the subscriber's public key,</li> <li>4. identifies its operational period, and</li> <li>5. is digitally signed by the certification authority issuing it.</li> </ol>
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates.
Commercial-Off-The-Shelf (COTS)	Hardware and software IT products that are ready-made and available for purchase by the general public.
Cross-Site Request Forgery (CSRF)	A type of Web exploit where an unauthorized party causes commands to be transmitted by a trusted user of a Web site without that user's knowledge.
Demilitarized Zone (DMZ)	A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks.
Denial of Service (DoS)	The prevention of authorized access to resources or the delaying of time-critical operations.
Distributed Denial of Service (DDoS)	A Denial of Service technique that uses numerous hosts to perform the attack.
Hash-based Message Authentication Code	A message authentication code that uses a cryptographic key in conjunction with a hash

(HMAC)	function.
Identification and Authentication (I&A)	The process of establishing the identity of an entity interacting with a system.
Intrusion Detection System (IDS)	Software that looks for suspicious activity and alerts administrators.
Intrusion Prevention System (IPS)	System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
Man-In-The-Middle (MITM)	An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them.
Message Authentication Code	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Metacharacter	A character that has some special meaning to a computer program and therefore will not be interpreted properly as part of a literal string.
Out Of Band	Used to refer to information transmitted through a separate communications channel.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Token	A physical object a user possesses and controls that is used to authenticate the user's identity.
Transport Layer Security (TLS)	An authentication and encryption protocol widely implemented in browsers and Web servers. HTTP traffic transmitted using TLS is known as HTTPS.
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act.
UOCAVA Systems	Information technology systems which support various aspects of the UOCAVA voting process?

XSS	Cross-Site Scripting (XSS) is a security flaw found in some Web applications that enables unauthorized parties to cause client-side scripts to be executed by other users of the Web application.
-----	---

**NISTIR 7682**

# **Information System Security Best Practices for UOCAVA- Supporting Systems**

Andrew Regenscheid

Geoff Beier

Santosh Chokhani

Paul Hoffman

Jim Knoke

Scott Shorter

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

[This page intentionally left blank. ]

**NISTIR 7682**

# **Information System Security Best Practices for UOCAVA- Supporting Systems**

Andrew Regenscheid

Geoff Beier

Santosh Chokhani

Paul Hoffman

Jim Knoke

Scott Shorter

September 2011



U.S. Department of Commerce

*Rebecca M. Blank, Acting Secretary*

National Institute of Standards and Technology

*Patrick D. Gallagher, Under Secretary for Standards and Technology and Director*

[This page intentionally left blank.]

## ACKNOWLEDGEMENTS

The authors, Andrew Regenscheid of NIST, Paul Hoffman of the VPN Consortium, and Geoff Beier, Santosh Chokhani, Jim Knoke, and Scott Shorter of CygnaCom, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. In particular, the authors would like to acknowledge Shirley Radack, Ray Perlner, Erika McCallister, Murugiah Souppaya, and John Wack of NIST, Matt Masterson, and James Long of the Election Assistance Commission, and Carol Paquette, Mark Skall, Tom Caddy and Karen Scarfone for their feedback on drafts of this document.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by organizations even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, organizations may wish to closely follow the development of these new publications by NIST.



## Table of Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>1 INTRODUCTION .....</b>	<b>3</b>
1.1 PURPOSE AND SCOPE .....	3
1.2 INTENDED AUDIENCE .....	3
<b>2 OVERVIEW OF UOCAVA-SUPPORTING SYSTEMS .....</b>	<b>5</b>
2.1 SYSTEM OVERVIEW .....	5
2.1.1 Voter Registration and Ballot Request .....	5
2.1.2 Electronic Ballot Delivery .....	5
2.2 IT AND NETWORKING COMPONENT OVERVIEW .....	6
<b>3 IDENTIFICATION AND AUTHENTICATION .....</b>	<b>7</b>
3.1 AUTHENTICATING PEOPLE .....	9
3.2 AUTHENTICATING VOTERS .....	12
3.3 AUTHENTICATING SYSTEM ADMINISTRATORS AND ELECTION OFFICIALS .....	12
3.4 AUTHENTICATING JURISDICTION-ADMINISTERED SERVERS .....	13
<b>4 HOST PROTECTION .....</b>	<b>14</b>
4.1 TYPES OF UOCAVA HOSTS .....	14
4.2 PROTECTING VOTING SERVERS AND MANAGEMENT STATIONS .....	14
4.2.1 Management Access Control .....	15
4.2.2 Anti-malware .....	16
4.2.3 Configuration Management .....	16
4.2.4 Lifecycle Management .....	18
4.2.5 Secure Backup .....	19
4.2.6 Web Server and Application Security .....	20
4.2.7 Email Security .....	21
4.3 SPECIAL UOCAVA HOST CONSIDERATIONS .....	22
4.3.1 Protecting Data at Rest .....	22
4.3.2 Protecting Databases .....	22
4.3.3 Document Delivery Over Fax .....	23
<b>5 NETWORK PROTECTION .....</b>	<b>24</b>
5.1 TYPES OF UOCAVA NETWORKS .....	24
5.2 FIREWALL DEVICES .....	24
5.3 ENCRYPTION AND INTEGRITY PROTECTION .....	25
5.3.1 Common Cryptographic Protocols .....	26
5.4 AUTHENTICATION OF ENDPOINTS .....	27
5.5 CERTIFICATES, KEYS, AND TRUST ANCHORS .....	29
5.6 OTHER NETWORK PROTECTION .....	30
<b>6 ONGOING VOTING SYSTEM PROTECTION .....</b>	<b>31</b>
6.1 SYSTEM AUDITS AND RECORD KEEPING .....	31
6.1.1 Host Audits .....	32
6.1.2 Network System Audits .....	32
6.1.3 Log Security .....	33
6.1.4 Local Policy Audits .....	33
6.2 QUALIFICATIONS AND TRAINING .....	33
6.3 INCIDENT RESPONSE PLANNING .....	34
6.4 MEDIA CONTROL .....	35
6.5 CRYPTOGRAPHIC VALIDATION OF HOSTS AND NETWORK EQUIPMENT .....	35
<b>7 REFERENCES .....</b>	<b>37</b>
<b>8 GLOSSARY .....</b>	<b>38</b>

## Executive Summary

The *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA) protects the absentee voting rights for U.S. Citizens, including active members of the uniformed services and the merchant marines, and their spouses and dependents who are away from their place of legal voting residence. It also protects the voting rights of U.S. civilians living overseas. Federal, state and local election administrators are charged with ensuring that each UOCAVA voter can exercise the right to vote. In order to meet this responsibility, election officials must provide assorted mechanisms that enable voters who are away from their residences to obtain information and descriptions about voter registration and voting procedure, and how to request, receive, and return their ballots. UOCAVA also establishes requirements for reporting statistics on the effectiveness these mechanisms to the Election Assistance Commission.

In order to streamline the process of absentee voting and to ensure that these voters are not adversely impacted by the transit delays involved due to the difficulty of postal mail delivery around the world, Information Technology (IT) systems can be used to facilitate absentee voting in several ways. They can:

- Distribute information about the process of applying for absentee ballots, including eligibility requirements and application forms.
- Distribute information about the facts relating to specific elections, including dates, offices involved and the text of ballot questions.
- Collect completed voter registration applications.
- Inform voters of their registration status.
- Provide ballot tracking information.
- Distribute blank ballots.
- Maintain statistics used to prepare the UOCAVA-mandated reports.
- Maintain absentee voter registration information used to distribute ballots.

IT systems used to provide these functions face a variety of threats. If IT systems are not selected, configured and managed using security practices commensurate with the importance of the services they provide and the sensitivity of the data they handle, a security compromise could carry consequences for the integrity of the election and the confidentiality of sensitive voter information. Failure to adequately address threats to these systems could prevent voters from casting ballots, expose individuals to identity fraud, or even compromise the results of an election.

This document offers procedural and technical guidance, along with references to additional resources, to assist jurisdictions with the secure deployment of these systems. The guidance found in this document focuses on IT systems used to support remote voting but does not define a specific architecture or configuration.

## **Component and system selection guidance**

The security features outlined in this document rely on components that are frequently, but not always, found in commercially available IT products. In some cases, a product may appear to offer a feature but fails to support the options required for secure operation. Many of the practices required for secure operation are relevant to both IT systems as a whole and to the individual discrete components that may be used to build these systems. As a result, it is important that organizations or individuals responsible for selecting the IT products that will be deployed to support UOCAVA voting understand these components and the features required to implement them both when purchasing a turn-key system or selecting components to assemble into a system.

## **Component and system configuration guidance**

In most cases, the IT products used to support absentee voting will be general-purpose commercial products suitable for a wide variety of applications with widely differing security requirements. As such, these products will be highly configurable. Many of the options offered by these products are not appropriate for every application, and could result in a security posture that is insufficient for a critical system or for one that contains sensitive data.

The guidelines in this document aim to assist system designers and administrators in two ways. First, as systems and components are configured for operation, this document lists sets of controls and configuration options that are critical to system security. Second, this document lists options for security controls which jurisdictions can use to help meet their security objectives for voting applications. The configuration practices found in this document aim to ensure that selections appropriate to the criticality and sensitivity of the systems are made, and address all security-critical facets of configuration. Jurisdictions will have customized their configurations depending on the architecture or implementation of their remote voting system.

## **Operational Guidance**

Finally, both technical and procedural controls are critical to securing these systems in operation. Organizations operating IT systems in support of UOCAVA voting should have comprehensively detailed security procedures for bringing the systems to a secure operating state, maintaining that secure state during operation, and securely terminating operations.

The guidance in this publication will assist election officials in collaborating with system designers and administrators to define system roles and establish processes that ensure the ongoing secure operation of the systems. It should also be consulted by system designers when documenting system operations and administrators when assigning individuals to fulfill roles defined by the system design.

# 1 Introduction

State and local election officials have various responsibilities under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), many of which involve information security. These state and local jurisdictions have begun to use information technology (IT) systems and the Internet to facilitate UOCAVA voting; for example, they are required to make voter registration, absentee ballot applications, and general election information available electronically. These IT systems are often used to distribute election information to voters, send and collect voter registration and ballot request forms, and deliver blank ballots.

## 1.1 Purpose and Scope

This document provides voting jurisdictions with security best practices for IT and networked systems that are used to support UOCAVA voting by sending or receiving voter registration or ballot request materials, or by delivering blank ballots to voters. Some of these best practices are unique to voting systems, but most are similar to, or the same as, best practices in IT and networked systems in general. For the latter, this document summarizes and points to other security-related documents published by NIST.

This document follows NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems*, which documents the threats to UOCAVA voting systems using electronic technologies for all aspects of the remote voting process. While NISTIR 7551 discusses high-level security controls capable of mitigating threats, the focus of that report was identifying technologies and associated risks. This document complements NIST 7551 by providing security best practices to help jurisdictions create UOCAVA voting systems based on security practices used in other IT applications.

The practices described in this document are broadly applicable to voting systems supporting UOCAVA that rely on IT systems, most of which run over the Internet. They supplement the other safeguards already in use in those voting systems, and possibly replace those practices that are out of date.

There are some topics not covered in this document. Remote voting techniques such as remote voting kiosks and voting over the Internet from personal computers, and using secure email such as S/MIME and OpenPGP for electronic ballot return, are out of scope because they are rarely used in UOCAVA voting systems and have a very different set of security challenges than the systems described here.

## 1.2 Intended Audience

This document is aimed at IT administrators who are implementing or maintaining systems that support UOCAVA. This includes technical support staff at state or local jurisdictions, vendors of products aimed at supporting UOCAVA voting, and service providers that host UOCAVA voting systems. The reader is assumed to have a medium to high degree of technical literacy of computers and networking.

This document refers to system designers, implementers, operators, auditors, and administrators as roles relative to the system used to support UOCAVA voting. Those terms may not directly correspond to job titles within the organization(s) assembling, procuring, deploying or maintaining these systems. For example, an individual who holds the title "System Administrator" in an organization's IT department may be charged with designing and deploying a system that sends blank ballots via email.

## **2 Overview of UOCAVA-Supporting Systems**

### **2.1 System Overview**

There are many different ways to support UOCAVA voters, and each jurisdiction must put together its own system for such support. This document covers some common parts of UOCAVA system architectures, and shows how to secure those parts against both normal and extraordinary threats. The two components that are covered in most detail are Internet-based or Internet-assisted delivery of blank ballots and voter registration.

#### **2.1.1 Voter Registration and Ballot Request**

In most jurisdictions, overseas and military voters must register in the jurisdiction where they are eligible to vote absentee in order to be qualified to vote in future elections, although some jurisdictions waive registration for military voters. A common method for voters to submit this information is the Federal Post Card Application (FPCA), a standard federal form that all states are required to accept. In addition, each state has its own registration form that reflects its specific registration requirements. Both the state specific forms and the FPCA request the following information from voters: name, date of birth, sex, race, home address and political party preference. They also ask for various forms of contact information, including telephone number, fax number, e-mail address, and mailing address.

Many jurisdictions make voter registration and ballot request forms available on their web sites, or are willing to e-mail them to voters upon request. Depending on local procedures and state law, some jurisdictions will accept completed voter registration or ballot request forms from voters over e-mail or allow voters to upload scanned forms to web sites. A growing number of jurisdictions are creating web sites that allow voters to fill out a web form to submit updates to their voter registration information. In these cases, proper operational, managerial and technical security controls must be implemented to ensure sensitive personally-identifiable material from voters is kept secure.

#### **2.1.2 Electronic Ballot Delivery**

Blank ballots are sometime created in electronic format and delivered to voters electronically. In UOCAVA environments, electronic delivery of ballots over the Internet overcomes many of the obstacles of delivering paper ballots in a timely and verifiable fashion. Such ballots are commonly formatted as PDF files which the voter can print locally and return by postal mail.

Blank ballots can be delivered to voters by email or over the Web. The choice of how to deliver ballots involves many variables. Some considerations include:

- Some jurisdictions have recent email addresses of non-local voters, making email delivery possible.

- Ballot availability may be restricted based on the ability to authenticate the voter
- Local policy might require that ballots be encrypted for delivery

Note, this document only covers delivery of blank ballots to voters, not electronic voting itself (i.e., ballot return). Thus, it is expected that voted ballots described within this document will be printed and sent back to the jurisdiction via postal mail.

## **2.2 IT and Networking Component Overview**

Different voting systems have different computing and network components, but most have many components in common. They include:

- Computers used as web and email servers (as well as other public services)
- Server software and jurisdiction-specific configurations
- Network devices such as routers and firewalls
- Identification and authorization systems
- Shared networks, particularly the Internet
- Desktop and laptop servers used to manage other elements of the voting system

These elements are described in more detail in the remainder of this document based on their interactions with the security requirements discussed.

### 3 Identification and Authentication

A primary goal of voting systems is to ensure that every ballot is cast by a legitimate voter. Authentication is the process of establishing confidence in the claimed identity of a user or system. Establishing the identity of a user is critical to the security of the system since the authenticated identity forms the basis for what actions can be performed on the system and what information may be accessed. In addition to authenticating voters, every IT system used to support UOCAVA voting will have other classes of users, particularly administrators, who have their own set of rights and privileges on the system.

The strength of authentication necessary depends on the consequences of an authentication error. As such, users with more privileged levels of access should, in general, be authenticated with a higher level of assurance. For example, three likely classes of users on an IT system supporting UOCAVA voting are system administrator, election officials, and voters. Having insufficient authentication for a system administrator can have a much more negative effect on an election than having insufficient authentication of a particular voter because the system administrator has heightened privileges that allow them to affect the validity of votes from many voters.

Identification and authentication in face-to-face environments are quite different than in electronic environments. In most cases, electronic authentication (particularly over the Internet) gives much less assurance than in face-to-face environments. For example, seeing a person who is holding a government-issued photo identity card such as a drivers license or passport gives much more assurance than seeing a copy of the photo identity card that was emailed. It should be noted that face-to-face voting normally employs much less stringent verification on government-issued identification than other environments, such as in aviation security screening. Still, physical interaction with physical identification such as drivers' licenses gives a greater opportunity for better authentication than online systems.

In this discussion, the person who is asserting his or her identity is called the *claimant* and the party trying to assess the authenticity of the identity is the *verifier*. NIST SP 800-63 Rev. 1, *Draft Electronic Authentication Guideline*, provides guidelines for implementing electronic authentication that is used over open networks such as the Internet. It defines levels of assurance that are associated with various forms of authentication and lists the types of authentication that a verifier might use for authenticating a remote user's identification. Electronic authentication relies on *tokens*, which are either information that is only known to the person and the verifier, or a hardware device that can generate information that the verifier knows can only come from that device. A summary of the types of tokens that could be used in UOCAVA systems is:

- Handwritten signatures – This is the same type of token used by jurisdictions to authenticate local voters. Because it is easy to photocopy



signatures, it is common to require that signatures used for authentication must be original signatures, not copies (i.e., signatures used for authentication purposes must be “wet signatures”).

- Passwords – These are commonly short strings of letters, numbers, and possibly punctuation that the claimant is expected to memorize or to have stored in a password management tool. Section 4.3 of NIST SP 800-118, *Guide to Enterprise Password Management*, describes password management tools and their uses. Numeric PINs are a type of password that are all-numeric and often shorter than typical passwords.
- Identifying prompts – These are usually questions whose answers are known to few people, including the claimant, such as “what city were you born in” or “your first pet’s name,” and are often only used for low-value authentication.
- Printed sets of secrets – This might be a sheet of paper or a small booklet that is unique to each claimant and which contains numerous secret values. The verifier prompts the claimant to reveal one of the values by its position (such as “enter the number that is in the second column in the tenth row of page 5”).
- Out-of-band hardware access – This type of authentication relies on the claimant having their own hardware that the verifier can initiate communications to. For example, if the claimant registered a phone number with the verifier ahead of time, the verifier can tell the claimant a secret, and then call the claimant on the registered phone number and ask for the secret.
- Single-factor One Time Password Device – These hardware devices spontaneously generate new passwords on-demand or at set intervals, and display them on the device. Users of single-factor one time password devices do not need to unlock the device before it will generate passwords. These devices are typically used in combination with other types of authentication tokens. For example, the verifier might authenticate the claimant by asking for the correct memorized password and one-time password.
- Multi-factor One Time Password Device – These hardware devices generate new one time passwords only after being unlocked by the claimant. For example, the claimant might unlock the multi-factor one time password device by entering a PIN directly onto the device, or using a biometric (e.g., fingerprint) reader on the device. Typically the one time password generated are displayed on the device and manually input into another system by the claimant for transmission to the verifier.
- Cryptographic Software – These are cryptographic keys that are stored on disk or some other unprotected media that typically must be unlocked before use (e.g., using a password). For example, the cryptographic keys might be stored in an encrypted format, using passwords to decrypt them.

Authentication is accomplished by having the claimant interact with the verifier using a cryptographic protocol.

- Cryptographic Hardware – These devices contain a protected cryptographic key that typically must be unlocked before use (e.g., using a PIN or biometric). These devices usually use the cryptographic key to digitally sign challenges from the verifier. A smart card is a common type of a hardware cryptographic hardware device.

Agreeing on the type of token that will be used for future authentication is called *issuance*. Issuance normally happens in person because of the chicken-and-egg problem of not being able to authenticate a request for issuance. However, one can use one token to authenticate a request for another. It is quite common to use a handwritten signature as authentication for a request for a token that can be used for electronic authentication when in-person issuance is not possible.

### 3.1 Authenticating People

The jurisdiction is the verifier when authenticating voters and people who act in administrative role. The jurisdiction and the claimant must agree on the mechanism for authentication before a voter asks to perform an action that requires authentication (such as changing their registration information).

All authentication mechanisms require that the verifier keep some record of what was presented by the claimant (e.g., the handwritten signature) or given to the claimant (e.g., the one time password generator) at the time of issuance. When authenticating, the verifier compares what is presented with that original information.

If the authentication mechanism is a handwritten signature (as in the case of non-electronic voting), the issuance information is an original signature or a copy thereof. Even if someone who wants to impersonate the voter sees the signature or copy, they still have to reproduce it in a wet-signed duplicate, which is considered hard; this is why bank checks have worked as well as they have for over a hundred years. Note, however, that banks currently do not rely solely on visual inspection of signatures for validation of checks, and modern signature verification tools use machine learning algorithms that are rarely used in voting contexts.

The following shows likely considerations for authenticating voters with the different types of authentication systems:

<b>Authentication type</b>	<b>Security Considerations</b>	<b>Deploying and Verifying</b>
Handwritten signatures	Currently universally used for in-person voting transactions, thus strong enough for remote transactions.	If a ballot or information update form is delivered electronically, the claimant needs to have access to a printer. The claimant needs to be able to send the wet-signed paper to the verifier.
Passwords	Users often use the same passwords at multiple sites and/or choose weak passwords, making impersonation attacks fairly easy. No hardware is required, making this the easiest electronic token available.	Password can be chosen by the claimant or the verifier. Storing or transmitting unencrypted passwords makes attacks easier.
Identifying prompts	Generally not used for voting systems because the answers may be easy to guess or may be easy to determine from public systems.	Prompts need to be chosen by the verifier. Storing unencrypted prompt responses makes attacks easier. Normally more than one type of prompt is used in a single system.
Printed sets of secrets	Can be made secure against impersonation attacks by having the secrets be at least 40 bits long; these secrets are still easy to type.	Verifier must get the printed material to the claimants, and claimants must have the material available when asserting their identity. Storage of secrets and prompts should be encrypted.
Out-of-band hardware access	The verifier must assume that the hardware being accessed is still controlled by the claimant. For example, if the claimant has lost their cell phone, the new possessor can impersonate the claimant.	A second communication system (such as a phone system) must be deployed and available to people who are doing the verification.

Single-factor One Time Password Device	These are usually small, hand-held cards and therefore can be lost or stolen. If these used as the only authentication factor, the new possessor could impersonate the claimant. Therefore, these should be used with another authentication factor, such as a memorized password.	The claimant needs to be able to receive a short prompt and, within less than a minute, access the device and repeat back a short message from the device to the verifier.
Multi-factor One Time Password Device	These are usually small, hand-held cards and therefore can be lost or stolen. The new possessor has to be able to unlock the device (e.g., by guessing the PIN) in order to impersonate the claimant.	The factor used to unlock the device must be set prior to deploying the device. This could be having users set or memorize a PIN, or having the device learn a biometric.
Cryptographic Software	The security of the authentication mechanism depends on claimants keeping their private keys secret.	The claimant needs to possess the private key, and the verifier needs to trust that the public key associated with the private key belongs to the claimant. Private keys are usually protected with passwords.
Cryptographic hardware devices	These are usually small, hand-held cards and therefore can be lost or stolen. Many of these cards are protected with PINs or passwords; the new possessor has to be able to guess the password in order to impersonate the claimant. When implemented properly, this is a very strong authentication mechanism.	The claimant needs to have a device that reads the cryptographic device (e.g., a smart card and card reader) connected to the computer they are using while authenticating.

### 3.2 Authenticating Voters

A potential voter's identity needs to be authenticated before they can cast a ballot in an election. Election jurisdictions have always had methods for identifying and authenticating voters at polling places. Voting remotely, such as is enabled by UOCAVA, changes the ways that people are identified because the voter is not seen in person. Jurisdictions have typically authenticated absentee ballots submitted by UOCAVA voters using hand signatures, but may use forms of electronic authentication as they deploy electronic and Internet-based delivery methods for election materials. Establishing trusted agents to perform in-person ID verification for voter credentialing for remote (particularly overseas) voters is difficult and may be beyond the capabilities of a particular jurisdiction office.

As described in Section 1, this document does not cover the case of electronic ballot return by voters. Jurisdictions may, however, require authentication of a person's identity for actions other than voting. For example, jurisdictions may require authentication of identity before allowing someone to change the information stored for a registered voter. While it is more common to authenticate marked ballots once they've been returned, some jurisdictions may wish to also authenticate potential voters prior to sending them blank ballots. For many jurisdictions, remote electronic authentication of voters will serve as a secondary authentication mechanism, with handwritten signature verification on returned ballots serving as the primary authentication mechanism.

Like banking web sites, most jurisdictions use passwords for authentication, even though these are considered fairly weak in the security community. Passwords are familiar to users, do not require use of special hardware by the voter, and can be used in a variety of locations. The security risk of using passwords for authentication is high but can be mitigated. NIST SP 800-118, *Guide to Enterprise Password Management*, describes the use of passwords; Section 3 of that document describes threat mitigation in great detail. As noted there, one of the best mitigation strategies is for passwords to be assigned by the verifier because the verifier can use rules for creating passwords that are likely to be much more secure than those that are typically chosen by the people who will use them.

If the authentication mechanism is a password, the jurisdiction has multiple choices for how to store the issuance information. They can store the password just as it was entered, but if the file in which the password is ever compromised by an attacker, that attacker can impersonate the voter with no effort at all. Because of this, most security-aware organizations who store passwords for verification do so by repeatedly encrypting the password with another value. If an attacker accesses this file, they must perform much more work to retrieve the password.

### 3.3 Authenticating System Administrators and Election Officials

The tradeoffs for authenticating people who manage voting systems are quite different than those for authenticating voters. Many of the types of device-based

tokens that are difficult in practice to distribute to voters, particularly remote voters, have much better security properties than passwords. Any small difficulty associated with distributing and administering these better mechanisms may be outweighed by their better security. That is, even if it is not terribly convenient for a system administrator to need to use a device-based authentication mechanism, doing so protects a system that itself protects the validity and secrecy of elections.

Note that different voting systems allow different types of authentication tokens. Many (but, unfortunately, not all) systems allow one or more types of strong authentication for administrative access. Jurisdictions that produce their own voting systems can choose one or more of these types of authentication in their designs. It is important to remember that role-based authorization (such as giving different rights to a system administrator than to an auditor) can be based on different types of authentication; people whose roles require less security can use authentication mechanisms that are easier to deploy.

### **3.4 Authenticating Jurisdiction-Administered Servers**

Users need to authenticate the servers that they connect to so they can be sure that the information they receive comes from the source that they expect. Essentially all server authentication today is done with digital signatures through the TLS security protocol.

When a voter uses the Internet to connect securely to a server that they think is administered by a jurisdiction, they use their web browser and TLS. The first steps in that protocol are to authenticate the server to the user by comparing the domain name that the user accessed with the name in the certificate presented by the server in the TLS handshake and to be sure that the server knows the secret key associated with the certificate. The voter's browser then checks if the certificate is issued by a trusted certificate authority (CA) and, if so, allows the user to proceed securely to the intended web site. Note that there is a serious but unsolved problem with the extremely large number of CAs and the fact that CAs do not incur almost any liability if they issue erroneous certificates that could mislead voters into trusting that they were on a jurisdiction's site when in fact they were led somewhere else.

## 4 Host Protection

The two major parts of an electronic voting system that need to be protected are the computers (hosts) on which processing happens and the network that is between those computers. This section covers how to protect the computers; Section 5 covers how to protect the network. Both parts of an electronic voting system also have ongoing protection such as audits and policy reviews; these are covered in Section 6.

### 4.1 Types of UOCAVA Hosts

UOCAVA hosts fall into two broad categories:

- Hosted voting system servers – Voting system servers are those with which voters interact. A common example of these is web servers that voters connect to from their personal computers to get voting information, request paper ballots, get electronic ballots, and update their registration information. If a jurisdiction contacts voters through email, the email server used to send messages would also be a hosted voting system server.
- Management stations – These are systems that only jurisdiction IT and network administrators interact with. Typically, these hosts are used to manage and monitor hosted voting system servers, networks, and personal computers used by jurisdiction employees. Note that these management stations may manage and monitor both UOCAVA and non-UOCAVA systems at the same time.

Both hosted voting system servers and management stations may be local to the jurisdiction or may be remote (particularly, overseas) but controlled by the jurisdiction through contracts with service providers. In fact, if the jurisdiction has outsourced some of its IT functions, the management stations are likely to be owned and controlled by contracted company, not the jurisdiction.

The difference between the two types of hosts is due mostly to who can access them. Hosted voting system servers are by design accessible to Internet users, whereas management stations are often on networks that are protected by firewalls. Note that not all management stations are on protected networks: a common example is a PC used by a jurisdiction IT staff to manage systems from home or while travelling.

Protection of personally-owned PCs used by voters and remote voting kiosks are not covered here. The vulnerabilities associated with these systems, and the mitigations for those vulnerabilities, are quite different than what is described in this document.

### 4.2 Protecting Voting Servers and Management Stations

Voting system servers and management stations can be vulnerable to a wide variety of attacks from the Internet. Servers are normally at fixed, easily-determined locations, which makes a prolonged attack easier to mount. Management stations at fixed locations that are not protected by a firewall have a

similar attack profile. In fact, management stations that are fully protected from the Internet can still be the target of attack if another computer on the protected network is compromised, such as by malware that was delivered in email or by web browsing.

Jurisdictions that have voting servers and management stations that can be reached from the Internet need to assume that attackers will want to take control of these computers, even if the attacker is uninterested in the voting aspect of the system.

#### **4.2.1 Management Access Control**

Computer management entails any modification to the computer that changes the way that the computer operates. *Management access control* is restricting who can manage the computer to a limited number of known people.

For example, on a PC used in a personal work setting, setting the electronic clock back by an hour will have minimal impact on the use of the computer; on a server that is handling requests for electronic ballots, making such a change (even with auditing) could have huge effects on the security of the voting system. Other management tasks can similarly be benign or serious; changes such as rebooting, patching the operating system, limiting the ability of a user to write files over a certain size, or even where DNS resolution information is obtained need to be considered in light of all the operational uses of the computer. Similarly, one might allow certain people rights to change only a few settings on a server, but it is almost impossible to prevent anyone from rebooting a computer if they have physical access to it.

Every server has at least one way to manage it, and often has at least a few. Some servers are managed directly on the server themselves, using keyboards and monitors attached directly to the servers. More and more, however, servers are managed by workstations (often regular PCs) that access them through local networks and/or the Internet. In the latter case, management access control for the server also means access control for any workstation that can manage the server through its remote interface. Thus, the scope of access control is often much wider than just that of the server itself. It is important to recognize that the management of any particular computer can be done in many ways, not just one.

Controlling management of servers requires attention to at least three areas:

- Minimize the number of users who can manage a computer to the bare minimum needed to reliably maintain the system. This is not as simple as it initially sounds: having too few administrators makes recovering from emergencies difficult because it may be hard to reach anyone who has management authorization, but allowing too many increases the risk that any one might be impersonated by an attacker.
- Use strong authentication for every user who is allowed to administer the computer. Use of passwords that might be easily guessed or copied from



other servers to which an attacker may have access is not strong enough for servers of high value.

- Record all logins to a server in a way that even an administrator cannot easily change. Anyone who can impersonate a user who has administrative privileges can often make changes that are difficult to trace unless reliable audit trails are kept.

Access control goes well beyond these three topics, but implementing them greatly reduces exposure to typical attacks on servers and makes such attacks easier to detect and possibly fix.

#### **4.2.2 Anti-malware**

All server operating systems are susceptible to malware, although there is a wide range of vulnerability. Malware can be spread through many mechanisms, such as exploiting security holes in web browsers, mail attachments, and open services that have programming errors. The goal of almost every attacker is to get administrative access to the server; from there, they can change the system to allow later access.

Server operating systems that have a history of exploitation by malware usually have anti-malware available from the operating system's vendor, other vendors, or both. Using anti-malware on such systems is necessary for good server hygiene. However, installing anti-malware is usually barely sufficient for the task. Because attackers are constantly changing their malware, constantly keeping this anti-malware software up to date is also necessary. Some anti-malware software has daily updates, and all servers that use that software should update whenever there is a new release.

Note that not all server operating systems have significant malware problems, and thus there is little market for anti-malware on those operating systems. However, all operating systems have vulnerabilities that are discovered after release, and thus it is still necessary to perform updates on a regular basis. This is similar in concept to updating anti-malware, although the mechanism for updating operating systems is usually more cumbersome than updating anti-malware. Closing known vulnerabilities helps prevent exploitation by new malware that would not be detected by even by an up-to-date malware scanner.

Management stations are often normal PCs running specialized software that controls the voting servers. Normal PCs are often susceptible to the wide range of malware infecting the Internet. This leads to two main strategies for preventing management stations from getting and passing along malware: run anti-malware conscientiously and restrict the use of any software other than the management software.

#### **4.2.3 Configuration Management**

Changes to the configuration of a voting server can have significant consequences on all aspects of the voting system. For example, a change to the networking software could cause some previously-acceptable communication to be rejected

and previously-unacceptable communication to start being accepted. Another example is adding a piece of additional monitoring software: such a seemingly-benign change could slow the system significantly and/or possibly block the monitoring of existing software.

NIST SP 800-128, *Guide for Security Configuration Management of Information Systems*, provides guidelines for managing the configuration of systems such as servers and the networks on which they run. It emphasizes the need to keep records of baseline configurations (known-good starting points in the lifetime of a system) and maintaining configuration management plans, particularly with respect to system security. Section 2.2 of SP 800-128 gives a good overview of the process of configuration management.

In the context of a voting server, a “configuration change” could be almost any change to the settings and applications running on the server, even those not necessarily associated with the voting software on the server. In addition, hardware changes, such as adding new memory or changing the network switch to which the server is connected, constitute configuration changes.

Thus, it is critical to start with a configuration that is both secure and is proven to work well as a whole (that is, all the software is known to work together). When the jurisdiction is sure that this configuration is correct, it is marked in the configuration management system as the baseline and changes to this baseline are then logged. NIST has created a set of checklists and benchmarks for a wide variety of software that can be used for creating baseline configurations. The checklists can be found on the NIST web site at <http://checklists.nist.gov/>, and the methodology used to create the checklists is described in NIST SP 800-70rev1, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*.

Further, it is critical to always track every change to any configuration on a voting server, even if the change initially seems inconsequential. The type of planning needed for this level of tracking is described in section 3.1 of SP 800-128. In order to be sure that all changes, even innocent-looking ones, are tracked, it is essential to limit the people allowed to make any sort of software change to those who understand configuration management and participate in the management tracking that has been instituted for the system in question. Normal software updates for both operating systems and application software inherently cause changes to a configuration. This does not mean that they should not be done, just that every such change be done under the control of the configuration management system with the ability to roll back to a known-good state if the changes stop the system from performing its task or inadvertently reduces the security of the system.

If new problems appear on the server, even after other changes have been applied, being able to look through the configuration change log can help pinpoint the changes that caused the problems; such monitoring is covered in section 3.4 of SP 800-128. There are many software packages that can be used to log configuration changes, but even keeping dated notes in a text file is better than

nothing. Any configuration management should be done on a server other than the one that is being tracked, or at least the change database should be backed up to a different server so a change that is disastrous does not also take down the configuration management system itself.

Note that some of the logging discussed here might also need to be audited. Even if the configuration data itself does not need to be audited separately, it at least made available to those who are auditing the overall system in which the computers participate. It is good to work with auditors to plan for audits well before they happen in order to reduce surprises during the audit process that will force major configuration changes.

#### **4.2.4 Lifecycle Management**

The lifecycle of servers and management stations is often easy to ignore, but it is an important to monitor as part of the protection of the systems. In some organizations, lifecycle management is also considered part of the configuration management of a system. NIST SP 800-64rev2, *Security Considerations in the System Development Life Cycle*, describes the processes that lead to sound lifecycle management.

Lifecycle management involves many people. Section 2.3 of SP 800-64rev2 lists the many people in an organization that might be involved with lifecycle management for hardware and software.

The lifecycle of the hardware portion of a server or PC includes acquisition, modification, and decommissioning. Hardware acquisition is usually not an important step, although some jurisdictions might require only US-manufactured hardware systems. Hardware modifications such as adding RAM or upgrading a hard drive can have important ramifications on the software that is running on the computer, and thus needs to be logged.

Hardware decommissioning is often the most important part of lifecycle management in that all data retained in the hardware must be destroyed before the hardware is disposed. A safe way to do this destruction is to do a secure full-disk erase of all hard drives in the system. Simply erasing all "user data" has been repeatedly proven to be an insufficient protection against exposure of sensitive data on systems. Many operating systems retain user data in "system data" files that would normally not be deleted if only deleting user data. Section 3.5 of SP 800-64rev2 lists many steps in decommissioning that are often overlooked.

The lifecycle of the software portion of a server or PC includes acquisition and modification, although rarely includes decommissioning. In this case, "acquisition" consists of two phases: purchasing and installation. Protecting a server during purchase is usually not an issue. However, Section 3.2 of SP 800-64rev2 describes how to perform risk assessment which is often overlooked in software purchasing. The methods used for installing purchased software, however, can have implications on security if the new software affects how previously-installed software performs. For example, adding software that

purposely restricts the ability to use other software, such as anti-malware, can cause security problems if the blocked software is actually part of the security setup for the server. Thus, it is very important to monitor the logs of all server software after installing new software to be sure that the older software continues to perform as expected.

Software updates (sometimes called *patches*) can affect not only the updated software but also other software on the system. This is particularly true for updates made to operating system software. Most modern operating systems include utilities that often have security holes and thus will be updated when general operating system updates are applied. These changes, which can be critical to the security of the server, may have negative effects on other software, particularly software that requires a particular version of the operating system or its utilities. In some ways, updating software is similar to adding new software to a system, and it is very important to monitor the logs of all server software after updating software to be sure that the all software on the system continues to perform as expected. Thus, the considerations from Section 3.4 of SP 800-64rev2 on the management of operations become particularly relevant.

Some electronic voting systems come as integrated solutions that contain both the hardware and software. The lifecycle management for these unified systems is in some ways easier because there is a single target for management. However, some of the operations that are performed by system integrators is harder to track and can have serious effects on the security of the systems. Unified solutions should not be considered "better" because of potential reductions in lifecycle management needs; instead, they must be seen as having different needs for lifecycle management.

#### **4.2.5 Secure Backup**

Making copies of the software and data on a voting server is a double-edged sword. It is required for stability but it exposes all the software and data to possible compromise. That is, each time there is a back up of a critical part of a voting server, that backup needs to be secured as well as the original server. This tradeoff can cause some organizations to not back up often enough to be useful in an emergency, but it can also cause other jurisdictions to use less-than-adequate security for their backups.

The security policies that apply to the voting server must also apply to all backups of sensitive data and applications on the voting server. This includes deciding who has physical access to the backups, who is authorized to read the data on the backups, who can make subsequent copies of the backed-up material, and who can read the data itself. Duplicating the policies for the original data for backup data is often easier than enforcing those policies because many organizations have different people handle their original data and their backups. In such cases, however, doubling the number of people who have access to backups may significantly increase the risk of the backup data being improperly exposed.

In order to assess the security of their backup system, jurisdictions need written backup procedures as part of the operational step of lifecycle management. These procedures list not only how the backup is made (such as what data is backed up and on what media), but also where and how the backups are stored and who has physical access to the backup media.

#### **4.2.6 Web Server and Application Security**

Many of the servers used by jurisdictions for assisting voting are web servers. Web servers are different than other Internet servers in that potential attackers have studied web servers in greater detail than application-specific servers. Thus, they have all the same security issues as generic servers that are exposed to the Internet, but are susceptible to greater attacks because of the acquired skills of a larger set of attackers.

Because of the widespread use of public web servers, NIST SP 800-42v2, *Guidelines on Securing Public Web Servers*, details the procedures that server administrators should follow in order to reduce the possibility of security flaws. For many organizations, flaws that expose private data (e.g., data associated with voters) are considered very damaging. For voting jurisdictions, flaws that allow an attacker to successfully impersonate a web server can be even more devastating because voters could be given incorrect information about how and where to cast ballots, which in turn can lead to flawed elections and loss of confidence from voters. Following the guidelines in SP 800-42v2, particularly those in Section 5 of that document, can go a long way towards reducing exposure to both errors and attacks on jurisdiction-run web servers.

Good web server hygiene is a complete field unto itself and much of it depends on the software that is chosen for the web server. Not only do different HTTP servers (such as Apache, Microsoft IIS, and Lighttpd) have different exposures to attacks, common additions to web servers (such as the PHP language and content management systems such as WordPress) also present their own attack possibilities. Some of the more important considerations in securing web servers include:

- Apply security patches for the web server software in use as soon as they are available. Web server vulnerabilities are tracked closely by the community of attackers, so applying patches in instances where a jurisdiction's server is vulnerable is critical to maintaining a secure system.
- Similarly, apply security patches for the additional web software packages in use as soon as they are available. These packages are easily detected by attackers and often can open the same types of attack vectors as the web server software itself.
- Constantly screen for cross-site scripting (XSS) vulnerabilities using firewalls and external screening services or web application scanners. Cross-site scripting is a mechanism for inserting scripts controlled by the attacker onto pages hosted on the web server. Their purpose is to gain access to private information that is used by the user's browser, particularly

site passwords and cookies. Most modern web browsers attempt to prevent cross-site scripting attacks by limiting the private information only to trusted web pages. However if an attacker can get their script onto a trusted page, they can masquerade as legitimate page content and access the private information.

- If the server accesses data from an SQL-based database, assiduously check all user input for *SQL injection* attacks. These attacks, which are still quite common on the Internet, look for web sites that pass insufficiently-processed user input to database back-ends and then send carefully-crafted input that will cause exposure of database records, and possibly allow destruction of databases.

Most voting web servers that send or receive sensitive information use the TLS protocol to cryptographically protect connections. TLS requires that every server have a certificate that contains its public key and an assertion from a trusted certificate authority (CA) that the public key is associated with the domain name used for the web server. The certificate used by a web server must not be expired and must be signed by a CA that is trusted by the user. Different web clients have different sets of trusted authorities, and this forces web server administrators to choose authorities that are trusted by all possible users of their secure web server.

A small number of voting jurisdictions use web services in Service Oriented Architectures (SOAs) for processing votes that were received electronically or were manually entered from paper ballots. NIST SP 800-95, *Guide to Secure Web Services*, lists many of the risks of using SOAs, and lists procedures that web services customers should take to protect themselves from loss of data confidentiality.

#### **4.2.7 Email Security**

Electronic voting systems may use email for sending ballots, sending election notifications, and other UOCAVA election materials. They may also use email for non-authenticated incoming mail, such as communications between jurisdictions and voting authorities.

Sending and receiving mail uses the SMTP protocol, which does not have any inherent authentication. NIST SP 800-45v2, *Guidelines on Electronic Mail Security*, describes the significant security issues that come with unauthenticated mail sending and receipt. Many SMTP servers support TLS for authenticating the server; that is, the initiator of an email exchange can authenticate the responding SMTP server using TLS with certificates. As long as both parties share trust in the same CA, the initiator can be sure it is communicating with the desired server. There is no common way to authenticate SMTP initiators. Using TLS with SMTP also provides encryption and integrity protection for the SMTP session.

The origin of messages sent over SMTP can be validated with three similar protocols: DKIM, SPF, and SenderID. Of the three, only DKIM is an Internet standard, and it is more widely deployed than the earlier SPF and SenderID

protocols. Note that these protocols do not provide encryption or integrity protection; instead, they only allow the sending organization to assert that mail messages that claim to come from a particular domain name in fact do so.

### **4.3 Special UOCAVA Host Considerations**

#### **4.3.1 Protecting Data at Rest**

Jurisdictions often store personally identifiable information (PII), voted ballots, and other private data on drives that need to be periodically backed up. The backed-up data must be protected with the same vigilance as the original data. If the original data is stored encrypted with keys of a certain strength and only usable by certain people, the backup needs to use the same strength keys (or stronger) and have the same access controls (or be even more restrictive).

Maintaining data covers two different topics: preventing unauthorized viewing of private information and maintaining the integrity of the stored data. The latter is extremely important for voting jurisdictions. The same tools used to prevent viewing of private data are also used to prevent changing of stored data by unauthorized parties, namely encryption and access controls. In this case, access control has two parts: access to viewing and updates. Normally, backups of data should never be updated; instead, the data is changed in its original location and a new backup is performed. This helps assure the integrity of the backups and keeps the access control rules clear, namely that people can only create new backups, not modify existing ones.

Protecting backups of data is complicated by the fact many backups are, by design, meant to be kept in a different location than the original data. In order to prevent loss of data due to a physical disaster such as fire in a data center, keeping off-site backups is a standard practice for most organizations. However, it is difficult to maintain the physical security of such backups identically as the original data because there are normally different staff at the storage site. Because of this, off-site backups should be encrypted with keys that are only known to people who have access to the original data.

#### **4.3.2 Protecting Databases**

Database servers, and the data they contain, have come under more frequent attacks in recent years. The personal data in registration databases, polling books, and so on, do not at first appear to be of value to typical Internet miscreants. However, all personally identifiable information (PII) can have value when combined with other data, such as stolen credit card numbers.

Protecting database servers is different than protecting web servers in that database servers are usually not directly accessed from the Internet. Instead, they are only accessed using custom programs running on web servers. However, this lack of direct connection to the Internet does not make them at all immune to attack. People looking to dump the contents of databases will try to fill in web forms in ways that will exploit bugs in the custom programs accessing the database servers.

It is common for attackers to try to inject database access commands in text fields in forms, hoping that the controlling programs are not scanning the input carefully before it is passed to the database server. In recent years, these *script injection* attacks have caused databases to reveal a great deal of personal information that the site operators thought was protected. To reduce the likelihood of script injection attacks:

- Rigorously check the values in every field of a web form, looking for any characters that should not be in that type of data, and also looking for patterns that look like database commands.
- Limit the number of fields that allow user input.
- Monitor the logs of the database server, looking for anomalous queries coming from the web server.

#### **4.3.3 Document Delivery Over Fax**

Many jurisdictions use facsimile (fax) systems to send and receive forms and voting information to UOCAVA and other remote voters. Nearly all fax transmissions are over standard telephone lines, which means that neither party can protect the network connection. Further, there is no widely-used standard for fax encryption. Thus, information sent by fax is at risk for possible interception or modification. Jurisdictions should carefully weigh the risks of fax transmission of election materials against the possible alternatives prior to using fax to send or receive sensitive information.

Some faxes are sent over the Internet, which would give them the same security properties as other documents sent over the Internet. However, most Internet fax systems are not end-to-end, meaning that the recipient still receives the fax on hardware connected to the phone system.



## 5 Network Protection

### 5.1 Types of UOCAVA Networks

The rapid expansion of the Internet and the continuing advancement of networking technologies has made defining particular network configurations more complicated. Networks in UOCAVA environments have the additional attribute of having long-distance components that are often not controlled by the election jurisdiction. This document covers the security practices for three types of networks:

- Links from remote to local systems run by election jurisdictions – These are sometimes dedicated leased lines, but could also be normal Internet links.
- Networks between end users and externally hosted voting systems – Some jurisdictions outsource operation of systems used to support UOCAVA voting. Typically, these systems allow voters to use whatever local Internet connection they have to connect to the voting system, and the voting system is connected over the Internet to the jurisdiction.
- Local area networks (LANs) – The security aspects of these are approximately the same as for other types of networks, although hardware switches can help in segmenting these networks.

### 5.2 Firewall Devices

In order to have any control of the data flowing through its network, an organization must make sure there are only a small number of connection points between the protected network and other networks. At each connection point, there should be a firewall device that controls both what comes in to the protected network and what goes from the protected network to other networks. NIST SP 800-41rev1, *Guidelines on Firewalls and Firewall Policy*, describes how to choose and deploy the firewalls that protect a network.

Section 3 of SP 800-41rev1 shows many typical network architectures and shows where firewalls fit into the design of protected networks. UOCAVA networks that are controlled by a voting jurisdiction, such as those between remote parts of a voting system or a LAN, are typical of the architectures people think of when deploying firewalls. However, most UOCAVA jurisdictions also must deal with remote users on their own computers accessing parts of a protected network, and thus the remote access to or through a firewall becomes much more important. Placement of firewalls in a network becomes extremely important because openings that are not protected by firewalls can lead to attacks on the network that are difficult to find and fix.

There are many types of firewall devices, some of which are more appropriate for protecting networks of devices that are all controlled by a jurisdiction, but others of which are more appropriate for allowing outsiders (in this case, voters and those interested in registering) to have limited access to some of the computers

in a protected network. Section 2 of SP 800-41rev1 describes each of the types of firewall devices that might be used. Jurisdictions that let voters have access to servers at the border or inside of its networks need to consider how to use web application firewalls and/or firewalls with network access control, and need to design their networks based on those choices.

Modern firewalls are fairly flexible and therefore complex devices. Most firewalls can implement a wide variety of security policies (such as "allow incoming traffic only to these hosts," "block all incoming traffic unless it is from this range of addresses," etc.). Section 4 of SP 800-41rev1 describes firewall policies and how they can be implemented in various firewall configurations.

After a security policy is established, each firewall at the perimeter of a protected network needs to be configured to meet that policy. If a network has multiple places where traffic from outside the network can enter and/or exit, that network needs multiple firewalls, each of which is configured with the same policy. Every firewall has a different method for configuration, which makes implementing multi-vendor networks difficult but not impossible. Even in a single-firewall network, it is important to be sure the configuration of the firewall fulfills all of the parts of the security policy.

It is common for organizations that have systems placed remotely, such as a voting jurisdiction that has overseas servers, to have multiple networks that need to be linked together. This linking is often done using firewalls to segment the network into smaller networks with connections between them. A firewall that inspects the source and destination of each packet can be used to keep a particular set of addresses on just one segment of a network. Segmented networks are not necessarily more secure than a single unified network, but they may be easier to administer. Network segmentation is covered in Section 3 of SP 800-41rev1.

### **5.3 Encryption and Integrity Protection**

Data that passes over public networks can be inspected and/or changed by various types of attackers. Such attacks can have a devastating effect on the organization that runs the network. For example, a voting jurisdiction that runs a UOCAVA network might have voter registration information and possibly even votes (e.g., the contents of mailed-in absentee ballots) passing over its network. An attacker who can change registration or voting information can potentially change the outcome of an election. Even if an attacker can only see this information, revealing that ability can greatly reduce the public's trust in the election jurisdiction.

To prevent such attacks, the public links in a network needs to be protected with cryptography. The two primary types of protection are encryption (the scrambling of data so an attacker cannot understand it) and integrity protection (preventing forged data from being accepted on the network). Encryption and integrity protection are usually provided at the same time. Even though it is technically feasible to have a network that provides integrity protection without

encryption and vice versa, most businesses want both, so they use a single network protection system that provides both.

Different cryptographic algorithms and different sizes of keys offer different levels of protection from attack. Therefore, it is important for an organization to be sure to use both the correct algorithms and the proper size keys for their needs. NIST's recommendations for the algorithms and key sizes that are acceptable to use to protect government data in non-national security systems are found in NIST SP 800-131A, *Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths*. Section 2 lists the encryption algorithms that are recommended; Sections 3, 5, and 6 lists the recommendations for key sizes. This document augments the advice given in NIST SP 800-57 Part 1, *Recommendation for Key Management – General*, and NIST SP 800-57 Part 3, *Application-Specific Key Management Guidance*. The former describes best practices for key sizes and cryptographic algorithms, while the latter talks about the type of key management that should be used in specific protocols such as IPsec and TLS.

Note, using encryption and integrity protection is appropriate between all types of networks, not just those that are connected with public links over the Internet. "Private" links such as leased lines can be snooped on and have their traffic changed by attackers; the only thing preventing this is a trust that the service provider has configured every router and switch between the ends of the link correctly. If there is a single mistake in the configurations, the traffic may be visible and vulnerable to modification.

### 5.3.1 Common Cryptographic Protocols

TLS is used to protect web-based traffic (that is, traffic run over the HTTP protocol).<sup>1</sup> TLS is widely used for protecting point-to-point traffic, notably between a web client and a web server. TLS provides both encryption and integrity protection. Many protocols other than HTTP can be protected with TLS as well, but for voting jurisdictions, TLS is almost exclusively thought of in terms of web traffic.

IPsec is the best-known protocol for protecting client-to-network and network-to-network traffic. IPsec is normally thought of as a protocol for virtual private networks (VPNs). A VPN creates a private data network while using public networks (typically the Internet) while providing both encryption and integrity protection to all data in the protected network. Most corporate firewall products include IPsec capabilities, making it much easier for a organization to connect their networks with IPsec at the same time as using firewalls to filter traffic. Note, IPsec can also be used to segment networks with cryptographic protection between each sub-network. Section 4 of NIST SP 800-77, *Guide to IPsec VPNs*, describes in detail how to use IPsec for secure network designs.

TLS/SSL can also be used to create VPNs, which are typically referred to as SSL VPNs. NIST SP 800-113, *Guide to SSL VPNs*, covers the technologies used in typical SSL VPNs. Section 2.2 of that document describes the common use cases

---

<sup>1</sup> TLS is the successor to SSL, and the two names are often used interchangeably.

for SSL VPNs, which are mostly for roaming access users, not fixed networks such as are typical in UOCAVA environments. In fact, SSL VPNs can be used in some of the same environments where IPsec VPNs are used, but they offer no greater security than IPsec VPNs. Choosing which type of VPN to deploy usually depends on the operational ease of use. If there are many remote access users with unmanaged PCs, SSL VPNs are often appropriate. If the network consists mostly or solely of gateway devices, then IPsec VPNs are usually more appropriate.

S/MIME is the most widely-used standard for digitally signing and/or encrypting email. Many email products come with S/MIME built in, and others have free S/MIME extensions that can be added easily. An email message that is signed with S/MIME before being sent can be checked by the recipient to be sure that no one has tampered with the message. A message that is encrypted with S/MIME prevents someone watching the network traffic from reading the body of the email message (although note the headers of the message are sent unencrypted). OpenPGP is a standard similar to S/MIME, and it is also widely used in email systems.

In order to use S/MIME effectively, both the sender and the receiver must share a mutually-trusted certificate authority (CA). There are many commercial CAs, although only some of them issue certificates for S/MIME. There are also many non-commercial CAs that might be used by UOCAVA voters, including the US Government and US Department of Defense CAs. OpenPGP software usually uses a very different trust model than S/MIME, and does not normally have certificate authorities; this makes it harder to use in UOCAVA systems unless the voting jurisdiction already has a trust relationship with numerous other OpenPGP users.

As described in Section 2 of NIST SP 800-49, *Federal S/MIME V3 Client Profile*, different mail software supports different features of S/MIME, and network administrators need to be careful all systems can read and generate the S/MIME messages that are required for any voter information sent through secured email.

## **5.4 Authentication of Endpoints**

Network security relies on at least one party in every communication being fully identified. In many cases, it relies on all parties being identified to the satisfaction of the other parties. In voting systems, these parties are most often human users (such as potential voters, system administrators, and auditor) and computer systems (such as web servers, email servers, and network infrastructure). Some methods for identifying human users and computer systems are similar, others are very different.

The identities of users and systems are verified using authentication mechanisms. In many voting applications, it is very important to identify the user or system you are interacting with in order to not disclose information to, or receive forged information from, the wrong entities.

A system may need to authenticate a user before granting them access to sensitive information or network services. For example, a voting jurisdiction probably wants to authenticate a person before allowing them to update their

ballot delivery information; some jurisdictions may even require authentication before delivering blank ballots. Another typical use is authenticating users before allowing administration of networking systems and equipment.

A user may need to authenticate a system before the user is willing to divulge personal information that can be used to impersonate the user later. For example, a user would want to be sure they are talking to a trusted server before the user gives his or her password or data used for password recovery such as their mother's maiden name. System-to-system communication often also relies on both systems being able to authenticate the others' identity.

Section 3 covered identification and authentication of users for both local access to machines and access to network resources. As described there, low-impact systems frequently use passwords over an encrypted channel to authenticate users. Medium-impact systems often require multi-factor to authenticate users. For high-impact systems, cryptographic hardware devices such as smart cards can be used to authenticate users.

Authenticating machines normally involves stronger forms of authentication mechanisms. Instead of passwords or multi-factor authentication, machine authentication is almost always done with cryptographic authentication mechanisms using strong keys stored on the system. A strong key is one that contains so much unpredictable material an attacker could not possibly guess the key even if he or she used phenomenally expensive systems for an extremely long time.

Machine authentication comes in two broad categories: those that use asymmetric public keys (such as digital signatures and public key encryption) and those that use shared secrets. Both can be equally secure for authenticating machines, but they are used quite differently in practice.

- Authentication based on public keys requires the verifier either have a copy of the public key or, more often, trust a third party that assures the public key given by the claimant is in fact theirs. The latter is how essentially all web browsers using TLS allow users to authenticate the servers to which they connect.
- Authentication based on shared secrets requires the two parties to have already exchanged the key they will use for communication. This exchange takes place out-of-band, meaning it uses a different protocol than the one being protected.

If an attacker can get a copy of a machine's authentication key, that attacker can impersonate the machine. In most current deployments, keys are stored on hosts on normal storage media such as hard drives. This relies on the security of the system to be as strong for protecting the keys as it is for protecting other system-critical information and processes. For example, most keys can only be read and written by someone who has the highest authorization access on a computer. Some high-impact systems store their keys in hardware using hardware security modules (HSMs). HSMs have much better properties to protect

the keys from being read by an attacker, but rely on operational changes that are too onerous for many organizations.

## 5.5 Certificates, Keys, and Trust Anchors

Network devices such as web servers, mail servers, and firewalls, are normally identified to other devices using the cryptographic methods described above. These methods most commonly use digital certificates for identification. In a small number of voting systems, most notably with secure email, people are identified with certificates. In short, a digital certificate is a signed assertion that the cryptographic key in the certificate is associated with a particular person or system. Users of certificates rely on trusted third parties (often called "certificate authorities" or "CAs") to make those assertions.

In order for identification using certificates to be trustworthy, the secrets that are associated with the keys in certificates must be kept private; otherwise, an attacker who knows the secret could impersonate the holder of the keys. This requirement puts a lot of pressure on individuals to do proper key management. The three parts of NIST SP 800-57, *Recommendation for Key Management*, describe the issues with maintaining the secrecy of keys and the use of certificates for identification. In specific, Section 2 of Part 3 of this series lists many best practices for using keys in certificates.

In order for systems such as web browsers to work with certificates, they must have a set of *trust anchors* that are trusted to associate cryptographic keys with devices and people. A trust anchor is the key for a certificate authority who issues certificates (or authorizes others to do so on its behalf). The set of trust anchors used by an application or operating system is called the trust anchor *store*. Trust anchor stores must be managed carefully because if an attacker can get its own key in the trust anchor store of an application, or if he can subvert the trust anchor that is already in an application's trust anchor store, the attacker can impersonate systems with whom the application communicates.

There are many different ways a CA might create a certificate for a web server or email user (the process is called *enrollment* although that term is rarely used on CA web sites). Because of this, when asking a CA to create a certificate for you, you need to first find their enrollment instructions and be sure they work for the web server or email client for which you want a certificate. Most often, the process involves telling your software to create a *certificate request*, delivering that certificate request to the CA, receiving email from the CA to validate you are authorized to request a certificate, performing that validation, and then receiving the certificate itself.

If your intended users do not already trust the CA with whom you have enrolled, those users must add a trust anchor for that CA in their web browser, email client, or operating system. Again, the steps to do this vary widely between different types of software. Also, note some users will be very hesitant to add a trust anchor because most software (for good reason) gives dire warning about adding trust anchors. In most cases, jurisdictions will be able to obtain certificates from a trust anchor supported by default in common browsers.

Jurisdictions that want to be able to validate signed email from military personnel need to install the trust anchor for the US Department of Defense Root CA. This certificate can currently be found at <http://dodpki.c3pki.chamb.disa.mil/rootca.html>.

## 5.6 Other Network Protection

Networks that have many individual users often want to limit who has access to the network, or at least limit access to certain parts of the network. This type of fine-grained admission to a network requires network access control, sometimes abbreviated NAC. NIST SP 800-46rev1, *Guide to Enterprise Telework and Remote Access Security*, particularly section 3 of that document, describes network access control systems and how they can be placed in a network to grant the specific access to users that a network administrator would want.

Security systems such as firewalls, VPNs, and network access control do not always succeed in the goal of keeping unwanted traffic from a network. Because of this, some network administrators deploy intrusion detection systems (IDSs) and intrusion prevention systems (IDPs) in parallel with firewalls to look for many different types of unwanted traffic. As explained in NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, these devices are useful in profiling the type of traffic coming onto a network and looking for common attacks. However, managing IDSs and particularly IDPs can be very labor-intensive because most networks have complicated and hard-to-predict traffic patterns, in that these devices need to produce a lot of logs in order to be useful.

As described earlier in this section, network segmentation can make management of each segment easier. Firewalls and VPN devices can be used to segment networks at their edges. In a LAN, however, network segmentation can be achieved more easily with managed switches. Low-end, unmanaged switches create fast connections based on traffic patterns, but managed switches also allow configuration to restrict access to certain ports (and therefore the networks connected to the ports) based on policies. Many managed switches allow access to a particular port based on authentication protocols using passwords and certificates. Managed switches cost much less than firewalls or VPNs, and they require much less setup and operational overhead to run.

## 6 Ongoing Voting System Protection

Maintaining the security of electronic voting systems takes more than just planning and one-time execution of preventative steps: security must be monitored and acted on throughout the life of the system. Sections 4 and 5 of this document give advice about how to plan for protecting hosts and networks in a voting system, and discuss some aspects of how to maintain security day-to-day. However, IT threats faced by election system usually evolve, so paying attention to security every day can be just as important as planning and proper initial setup.

### 6.1 System Audits and Record Keeping

The core practice for ongoing security is auditing of IT systems. Observing the statuses of the various parts of a system allows an administrator to find where the system is vulnerable to threats or, if not found ahead of time, the part of the system that was vulnerable to a successful attack. By their very nature, voting systems are subject to audits and record keeping to detect voter fraud. This section covers system audits and record keeping specific to host and network security that can be quite different than the type of attacks seen on non-electronic voting.

Some voting audits may also require IT system audits as one part of the overall audit. These voting audits will probably specify what type of auditing is needed for hosts and networks, but a jurisdiction should strongly consider going beyond the minimum required by voting audits for their IT auditing practices. Collecting more information can help detect attempted attacks that might be missed by collecting only the minimum amount of information required.

It is relatively rare to see an attack in progress and recognize it as an attack, so keeping records of all audits is necessary. Good record keeping is useful for finding when and where an attack happened, but also for finding patterns of unsuccessful attacks as part of ongoing assessments about how to improve the security of a system. The value of the latter should not be underestimated: auditing stored audits can be very valuable to preventing attacks that take research on the part of an attacker.

Monitoring events can happen either in an automatic, continuous fashion, or sporadically by people who look through event logs and so on. Continuous monitoring is far more reliable for capturing data that can be used to analyze or prevent attacks, but sporadic monitoring by humans is required to detect anomalous events missed by automated programs. It is impossible to say either how detailed continuous monitoring records should be or how often sporadic human monitoring should take place: such judgments depend on the nature of the voting system and the value of various attacks to the attackers. Section 3 of NIST Draft SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, describes the process needed for both automatic and sporadic monitoring of networked computer systems.



### **6.1.1 Host Audits**

The servers and personal computers that run in a voting network are as subject to attack as any system on the Internet. Thus, it is important to audit as much information in these systems as you would any other network-connected system. The types of information typically monitored in hosts include:

- User logins
- Running of administrative software
- Addition and removal of applications
- Patching of applications and the operating system

Hosts on voting systems may have additional IT-related auditing requirements, such as monitoring changes to voter databases or logging the number of requests for particular types of ballots.

### **6.1.2 Network System Audits**

Networks themselves are rarely audited. That is, it is rare to try to perform a complete capture and audit of all information flowing over a network connection. Instead, the systems that make up the network have their software and event logs audited. These systems include all types of routers and firewalls, and some jurisdictions will even monitor local switches. The types of information typically monitored in hosts include:

- User logins to management software
- Event logs from firewalls and intrusion detection systems
- All configuration changes
- Use of encryption for connections
- Patching of system software
- Changes to hardware subsystems

Users of networks sometimes add unauthorized systems to the network. A common example is users who sometimes add wireless access points in order to improve local connectivity. In fact, these can unintentionally allow outsiders to access the network in ways unanticipated by the network administrator. Another common example is computers that have not been vetted by the IT department being added temporarily, but still causing havoc.

To prevent such unintended additions, many network administrators will perform system scans to see all the computers and network devices on the network. They then compare the results of the scan with a known inventory of allowed systems. The presence of such systems should be logged before removing the system from the network (or allowing the system if, in fact, it conforms with the network security policy).

### **6.1.3 Log Security**

Network security audits themselves need to be secured because they contain information that can be used to attack a network. For example, a typical audit will tell an attacker what the system administrators did not see when being probed for vulnerabilities. As described in NIST Draft SP 800-137, auditing information is normally kept offline or on systems that have different access control mechanisms than the systems that are being monitored.

The audit logs for electronic voting systems can have even more stringent requirements than those of normal networked systems if they may contain information about voters that can be used to surmise those voters' votes. Although it is unlikely these hosts contain actual votes, there are types of information that represent voting patterns that may be considered sensitive. If a log does not contain any personally-identifying information about voters or votes cast, the security of the log should be as high as for the logs of normal in-person voting. However, if the logged data (even if it is summarized data) contains more than what is available for in-person voting, the logs should probably be as secure as the data itself.

### **6.1.4 Local Policy Audits**

Many jurisdictions have their own security policies. These policies sometimes apply only to the voting aspect of a jurisdiction, but are often inherited from the larger government agency of which the jurisdiction is just one part. Audits of the security practices of a voting jurisdiction may therefore involve separate compliance reviews for separate security policies. These audits can usually be done concurrently because the policies will often have large (usually intentional) overlaps.

## **6.2 Qualifications and Training**

It is important the jurisdictions designing custom Internet-connected voting systems use current best practices in security. This is also true for jurisdictions selecting such systems from vendors: it is not sufficient to believe that all vendors are using security best practices that apply to each jurisdiction. Security practices are implemented by jurisdiction staff and contractors, so having all of those people be able to determine which practices are best is the first step to their implementation.

Different positions have different roles and responsibilities for security. For example, a database administrator has different security objectives than someone who maintains the operating system for web servers used by the jurisdiction. It is thus important that all the security roles and responsibilities for every position are clearly defined and documented.

Once the security responsibilities are laid out, the jurisdiction must ensure that each employee or contractor is qualified for the position(s) they have. This involves determining if each person has the necessary skills and experience to conduct the specific jobs(s) they perform. Note that in typical jurisdiction, a single person will have multiple security-related roles.

When evaluating how well the technical qualifications that a person has are matched for the security skills needed for a particular role, many factors need to be taken into account. They may already have relevant, related experience in security-sensitive tasks such as operating and/or designing systems with security components; they may have certifications in security technologies; and they may have recent education or training without having the opportunity to use it.

A jurisdiction can actively help raise the level of security skills through training programs for all staff. Such security awareness and training programs can help everyone know the jurisdiction's policies and procedures. Section 3 of NIST SP800-50, *Building an Information Technology Security Awareness and Training Program*, describes how to design such a program, and the rest of the document covers important topics such as how to evaluate training programs after they have been implemented.

In addition, a jurisdiction can create or purchase targeted ongoing training for people in specific security-sensitive roles, as described in Section 2.3 of SP800-50. This can help assure that technical staff are proficient in the technologies with which they work. Training can also help election officials and their management understand the risk inherent in the decisions they make.

Some of the more intensive training programs can lead to certification for the trainee. There are a variety of certifications for security personnel from various independent organizations, and each certification has its own level of value and appropriateness for particular tasks. Some of the many types of security certifications include proof of skills such as:

- designing and selecting online systems in which security is an important factor
- day-to-day IT operations of systems with security components
- security management for executives such as Chief Security Officer (CSO)
- managing the security aspects of networking systems for specific hardware and software vendors
- writing software that has security aspects, particularly cryptography

The first two of these are the most valuable in planning for and deploying voting systems connected to the Internet, although it is difficult to directly map the claims of a certification system on many of the tasks that jurisdictions assign to staff and contractors.

### **6.3 Incident Response Planning**

Monitoring electronic voting systems is important for determining when something important has happened, but monitoring must be followed up with incident response. Note, incident response entails responding to known attacks and, just as significantly, responding to events that are even slightly suspicious.

The latter category is often overlooked because it causes a large number of “false positive” reports, but it is a critical part of attack prevention.

Section 2 of NIST SP 800-61rev1, *Computer Security Incident Handling Guide*, details the kinds of incidents for which responses are needed. It emphasizes the need for response planning, including setting up response teams and publishing the response plans so that everyone involved knows their responsibilities.

Although some of the recommendations at the end of the section are specific to US government agencies, most of them apply just as well to any organization that needs to deal with computer and/or network incidents.

#### **6.4 Media Control**

Many different types of data stored on a computer or network device can be of value to an attacker. Although it is much more common for attackers to try to access valuable data over the Internet, having direct unfettered access to the media on which the data is stored is of huge value to an attacker. Thus, it is critical the media on which the data is stored are not directly available to any attacker, even after these media have been taken out of use.

Similarly, all media used for backups must be stored with at least the same level of safety as is used for the live data. Safely storing backups is different than protecting media that are actively being used because actively-used media are in systems that themselves are usually physically protected. Backup media, on the other hand, are normally kept in unattended locations where many types of media are stored together. Anyone with access to the storage location may be easily able to access particular backup media. Given this problem, normal monitoring of backup media usually involves a plan for destroying old backups that are no longer used.

Controlling election media is also critical for preventing the injection of malware that can then be propagated to users of a jurisdiction’s online systems. It is very common for miscreants to use generally-trusted sites that are not adequately protected as launching points for hidden distribution of malware. To prevent being the source of such attacks, jurisdictions need to have close physical control and chain-of-custody tracking for all their electronic media and Internet servers.

#### **6.5 Cryptographic Validation of Hosts and Network Equipment**

Nearly all voting systems use cryptography for some of their security features. It is important the cryptographic functions in such systems conform to widely-accepted standards and are implemented using industry best practices. Such conformance assures systems are using algorithms that have been vetted by experts throughout the security field; this, in turn, reduces the likelihood of security breaches due to poorly-chosen cryptographic functions.

NIST’s FIPS 140 series of requirements and certifications is probably the best-known set of conformance and best-practice standards available. FIPS 140 is the anchor of a program at NIST called the Cryptographic Module Validation Program (CMVP). US government agencies purchasing equipment that uses cryptography are required to verify the cryptography is certified to conform to FIPS 140, and

other industries have also made FIPS 140 certifications into requirements as well. More information on CMVP and the FIPS 140 program can be found at <http://csrc.nist.gov/groups/STM/cmvp>.

Compliance with cryptographic standards is often considered a one-time check at the time of purchase or deployment, but it really should be part of ongoing audits. A vendor's systems can lose its certification, such as if there is a software or hardware upgrade that breaks compliance. Also, compliance specifications themselves can evolve, and a system that complied with an older version of a specification may not comply with requirements specified in the newer version. Thus, checking for certification should be done periodically as part of normal security auditing practices.

## 7 References

NIST SP 800-41rev1, *Guidelines on Firewalls and Firewall Policy*

NIST SP 800-42v2, *Guidelines on Securing Public Web Servers*

NIST SP 800-45v2, *Guidelines on Electronic Mail Security*

NIST SP 800-46rev1, *Guide to Enterprise Telework and Remote Access Security*

NIST SP 800-49, *Federal S/MIME V3 Client Profile*

NIST SP 800-57 Part 1, *Recommendation for Key Management – General*

NIST SP 800-57 Part 3, *Application-Specific Key Management Guidance*

NIST SP 800-61rev1, *Computer Security Incident Handling Guide*

NIST SP 800-63 Rev. 1, *Draft Electronic Authentication Guideline*

NIST SP 800-64rev2, *Security Considerations in the System Development Life Cycle*

NIST SP 800-70rev1, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*

NIST SP 800-77, *Guide to IPsec VPNs*

NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*

NIST SP 800-95, *Guide to Secure Web Services*

NIST SP 800-113, *Guide to SSL VPNs*

NIST SP 800-118, *Guide to Enterprise Password Management*

NIST SP 800-128, *Guide for Security Configuration Management of Information Systems*

NIST SP 800-131, *Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths*

NIST Draft SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems*

Checklists and benchmarks for creating baseline configurations:

<<http://checklists.nist.gov/>>

FIPS 140 and NIST's Cryptographic Module Validation Program (CMVP):

<<http://csrc.nist.gov/groups/STM/cmvp/>>

## 8 Glossary

*Authentication* - The process of establishing confidence in the claimed identity of a user or system

*Claimant* - The person who is asserting his or her identity

*Enrollment* - The process that a Certificate Authority (CA) uses to create a certificate for a web server or email user

*Issuance* - Agreeing on the type of token that will be used for future authentication

*Management control* - Restricting who can manage the computer to a limited number of known people

*Management stations* - Systems with which only IT and network administrators interact

*SQL injection* - Attacks that look for web sites that pass insufficiently-processed user input to database back-ends

*Tokens* - Either information that is only known to the person and the verifier, or a hardware device that can generate information that the verifier knows can only come from that device

*Trust anchor* - The key for a certificate authority who issues certificates or authorizes others to do so on its behalf

*Verifier* - The party trying to assess the authenticity of an identity

**NISTIR 7551**

# **A Threat Analysis on UOCAVA Voting Systems**

Andrew Regenscheid  
Nelson Hastings



[This page intentionally left blank. ]

**NISTIR 7551**

# **A Threat Analysis on UOCAVA Voting Systems**

Andrew Regenscheid

Nelson Hastings

*Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930*

December 2008



U.S. Department of Commerce  
*Carlos M. Gutierrez, Secretary*

National Institute of Standards and Technology  
*Patrick D. Gallagher, Deputy Director*

[This page intentionally left blank. ]

## TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>1 INTRODUCTION.....</b>	<b>3</b>
1.1 SCOPE .....	3
1.2 STRUCTURE OF THIS PAPER.....	3
<b>2 BACKGROUND.....</b>	<b>4</b>
2.1 UOCAVA VOTING PROGRAMS .....	4
2.1.1 FWAB.....	4
2.1.2 Electronic Transmission Service.....	4
2.1.3 Voting over the Internet.....	5
2.1.4 SERVE.....	5
2.1.5 Interim Voting Assistance System .....	6
2.2 CURRENT UOCAVA VOTING PROCESS.....	7
2.3 DIFFICULTIES IN THE CURRENT UOCAVA VOTING PROCESS .....	9
<b>3 UOCAVA VOTING PROCESS .....</b>	<b>10</b>
3.1 VOTER REGISTRATION AND BALLOT REQUEST .....	11
3.2 BALLOT DELIVERY .....	11
3.3 BALLOT RETURN .....	12
<b>4 DESCRIPTION OF TRANSMISSIONS OPTIONS.....</b>	<b>13</b>
4.1 TRANSMISSION OPTIONS .....	13
4.1.1 Postal Mail.....	13
4.1.2 Telephone .....	13
4.1.3 Fax .....	13
4.1.4 Electronic Mail.....	14
4.1.5 Web-Based.....	14
4.2 OPTIONS FOR VOTER REGISTRATION AND BALLOT REQUEST .....	15
4.2.1 Postal Mail.....	15
4.2.2 Telephone .....	16
4.2.3 Fax .....	16
4.2.4 Electronic Mail.....	16
4.2.5 Web-Based.....	17
4.3 OPTIONS FOR BALLOT DELIVERY.....	17
4.3.1 Postal Mail.....	17
4.3.2 Telephone .....	17
4.3.3 Fax .....	18
4.3.4 Electronic Mail.....	18
4.3.5 Web-Based.....	19
4.4 OPTIONS FOR BALLOT RETURN.....	19
4.4.1 Postal Mail.....	19
4.4.2 Telephone .....	20
4.4.3 Fax .....	20
4.4.4 Electronic Mail.....	21
4.4.5 Web-Based.....	21

<b>5</b>	<b>THREAT ANALYSIS METHODOLOGY .....</b>	<b>23</b>
5.1	THREATS.....	23
5.2	THREAT SOURCES .....	23
5.3	EFFORT .....	25
5.4	DETECTION .....	25
5.5	IMPACT .....	25
5.6	POSSIBLE CONTROLS .....	26
<b>6</b>	<b>THREAT ANALYSIS .....</b>	<b>27</b>
6.1	REGISTRATION AND BALLOT REQUEST .....	27
6.1.1	<i>Postal Mail</i> .....	27
6.1.2	<i>Telephone</i> .....	28
6.1.3	<i>Fax</i> .....	29
6.1.4	<i>Electronic Mail</i> .....	30
6.1.5	<i>Web-Based</i> .....	32
6.2	BALLOT DISTRIBUTION .....	34
6.2.1	<i>Postal Mail</i> .....	34
6.2.2	<i>Fax</i> .....	35
6.2.3	<i>Electronic Mail</i> .....	36
6.2.4	<i>Web-Based</i> .....	37
6.3	BALLOT RETURN .....	39
6.3.1	<i>Postal Mail</i> .....	39
6.3.2	<i>Telephone</i> .....	40
6.3.3	<i>Fax</i> .....	41
6.3.4	<i>Electronic Mail</i> .....	42
6.3.5	<i>Web-Based</i> .....	45
<b>7</b>	<b>SECURITY CONTROLS .....</b>	<b>47</b>
7.1	POSTAL MAIL .....	48
7.2	TELEPHONE TRANSMISSION .....	51
7.3	FAX TRANSMISSION .....	55
7.4	E-MAIL TRANSMISSION .....	58
7.5	WEB-BASED TRANSMISSION .....	63
<b>8</b>	<b>CONCLUSIONS .....</b>	<b>67</b>
8.1	REGISTRATION AND BLANK BALLOT REQUEST .....	67
8.2	DELIVERY OF BLANK BALLOTS .....	67
8.3	RETURN OF VOTED BALLOTS .....	68
8.4	SUGGESTED NEXT STEPS .....	69
	<b>REFERENCES.....</b>	<b>70</b>
	<b>APPENDIX: ACRONYMS .....</b>	<b>72</b>

## Executive Summary

The Election Assistance Commission (EAC), with the assistance of the National Institute of Standards and Technology (NIST), is researching electronic technologies that may help to assist overseas voting as defined by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). This report contains the results of NIST's research.

### ***Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)***

In 1986, Congress enacted UOCAVA, which states that U.S. citizens that are part of the uniformed services, merchant marines, and their families or citizens residing overseas are allowed to register and vote absentee for Federal office. Additionally, the Help America Vote Act of 2002 (HAVA) requires the EAC to study overseas voting, including methods for sending balloting materials to overseas voters [28]. Most states have their own legislation covering how UOCAVA citizens register and vote. Overseas voting is treated by most jurisdictions as absentee voting, applying the same procedures (e.g., deadlines for requesting absentee ballots and returning completed ballots) as for an absentee voter within the United States.

### ***Purpose of Report***

UOCAVA voting generally relies upon postal and military mail as the mechanism to distribute and receive election materials, but inherent delays in the delivery times to citizens overseas plus legislated windows of time between finalization of ballots and the election can result in UOCAVA voters being unable to participate in elections. This report therefore examines electronic transmission options (telephone, fax, e-mail, web) for UOCAVA voting that are in limited use or have been proposed as methods for improving UOCAVA voting, and analyzes the security-related threats to these transmission options. This report presents initial conclusions regarding the use of these electronic technologies and suggested next steps.

This report identifies issues and threats associated with transmitting election information by postal mail and the four electronic transmission options identified below:

- *Telephone* allows instant two-way communication between two users. Voter information can be communicated over the telephone network to or from the UOCAVA voter either verbally or by using the telephone keypad. For example, a voter could request election material by following a series of voice prompts and pressing numbers on the keypad.
- *Fax* allows users to transmit written or printed information to another party. Voter information can be scanned and transmitted over telephone networks to or from the UOCAVA voter. In some states, faxes are used as an alternative to postal mail, allowing voters or election officials to fax election forms or ballots to the other party. For example, an election official could fax a blank ballot to the fax number provided by the UOCAVA voter.
- *Electronic mail (e-mail)* allows users to send text and/or files from one computer to another over the Internet. Voter information could be sent as an e-mail message or as an

attachment to the e-mail. For example, blank ballots could be sent as PDF files attached to an e-mail.

- *Web-based voting* allows users to communicate by using websites accessible via the Internet. Voter information can be presented, downloaded, or transmitted by the UOCAVA voter through the use of web pages and interactive forms. For example, voters could download blank ballots from a web site.

### ***Initial Conclusions***

The report looks at three UOCAVA election functions:

- registration and ballot request,
- blank ballot distribution to overseas voters, and
- voted ballot return.

*Registration and ballot request:* Voter registration and requests for a blank ballot by the UOCAVA voter can be reliably facilitated and expedited by the use of any of the electronic transmission options. The associated threats can be mitigated through the use of procedural and technical security controls and do not pose significant risks to the integrity of elections. It should be noted that e-mail and the web present greater security challenges (similar to those encountered by e-commerce applications) than telephone and fax.

*Blank ballot distribution:* Distribution of blank ballots to the UOCAVA voter can be reliably facilitated and expedited by the use of fax, e-mail, or web transmission. The threats associated with using fax, e-mail, and web transmission can be mitigated through the use of procedural and technical security controls and therefore do not pose significant risks to the integrity of elections. (Telephone solely to deliver blank ballots is not considered in this report as a viable transmission option for blank ballot distribution.)

*Voted ballot return:* Sending completed ballots from UOCAVA voters to local election officials can be expedited through the use of the electronic transmission options. However, their use can present significant challenges to the integrity of the election. Use of fax poses the fewest challenges, however fax offers limited protection for voter privacy. While the threats to telephone, e-mail, and web can be mitigated through the use of procedural and technical security controls, they are still more serious and challenging to overcome.

### ***Recommended Next Steps***

A number of states already distribute blank ballots via fax or e-mail. However, at this time there are no guidelines documenting best practices for fax, e-mail or web distribution of ballots. Developing a best practices document could help improve methods for distributing ballots using these transmission methods, and potentially improve the procedures and technical controls already in place in states currently using these methods. In addition, registration and ballot requests can also take advantage of these distribution methods, but there are more threats when handling personal information from voters. Voted ballot return remains a more difficult issue to address, however emerging trends and developments in this area should continue to be studied and monitored.

# 1 Introduction

The Election Assistance Commission (EAC) requested that the National Institute of Standards and Technology (NIST) research technologies to enable uniformed and overseas United States citizens to vote, as required by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) [21]. Additionally, the Help America Vote Act of 2002 (HAVA) requires the EAC to study overseas voting, including methods for sending balloting materials to overseas voters [28]. This report contains the results of NIST's research into technologies to enable overseas voting by United States citizens.

## 1.1 Scope

A general overseas voting process model was developed based on current UOCAVA practices. This report identifies three stages to the overseas voting process: voter registration and ballot request, blank ballot delivery, and voted ballot return. It describes the processes in each stage, the types of information transmitted, and the security needs for that information. In addition, a discussion of the current technologies that could be used to transmit voting information between voters and election officials is provided. Using the overseas voting process model and current technologies for transmitting voting information between voters and election officials, NIST has developed a threat analysis based on the methodology found in NIST Special Publication (SP) 800-30 *Risk Management Guide for Information Technology Systems* [2]. As part of the threat analysis, mitigating controls for each threat are provided when possible. The mitigating controls for each threat provided in this report provide the basis for an effort to develop best practices for overseas voting systems, but do not represent a set of complete and testable requirements for overseas or remote voting systems.

## 1.2 Structure of this Paper

The remainder of this paper is organized as follows:

- **Section 2** outlines historical and current approaches for UOCAVA voting.
- **Section 3** describes the three stages of the UOCAVA voting process: Voter Registration and Ballot Request, Ballot Delivery, and Ballot Return.
- **Section 4** identifies five transmission options for election materials: postal mail, telephone, fax, electronic mail and web-based systems. Each option is described and a typical usage scenario is provided for UOCAVA election systems.
- **Section 5** describes the threat analysis methodology used in this paper.
- **Section 6** provides the results of the threat analysis on UOCAVA election systems using the transmission options identified in Section 4 to support the three stages in UOCAVA voting.
- **Section 7** describes security controls discussed in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, which can mitigate some of the threats identified in Section 6.
- **Section 8** offers conclusions based on the results from the threat analysis.



## **2 Background**

In 1986, Congress enacted Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) [21]. UOCAVA states United States citizens that are part of the uniformed services, merchant marines, and their families, or U.S. citizens residing overseas are allowed to register and vote absentee for Federal offices. For state and local elections, most states have state legislation covering how UOCAVA citizens register and vote absentee. UOCAVA stated that a Presidential designee should carry out the mandates specified in the legislation. On June 8, 1988, Executive Order 12642 “Designation of Secretary of Defense as Presidential Designee” assigned the Secretary of Defense the administrative responsibilities for UOCAVA. In turn, the Secretary of Defense assigned these responsibilities for implementing the UOCAVA to the Federal Voting Assistance Program (FVAP) within the Department of Defense (DoD).

### **2.1 UOCAVA Voting Programs**

#### **2.1.1 FWAB**

UOCAVA [20, 21] calls for a Federal Write-In Absentee Ballot (FWAB) covering elections for Federal offices (e.g., President/Vice President, U.S. Senator, and U.S. Representative). In addition to the FWAB, UOCAVA describes a Federal Post Card Application (FPCA) that allows citizens to request an absentee ballot for a federal election. The FVAP has made the FWAB and FPCA available at locations around the world including military bases, embassies, consulates, election organizations, and corporations as well as online electronically at their website [19]. In addition to distributing the FWAB and FPCA, the FVAP has conducted pilot projects to investigate using electronic means, such as email and websites, to assist uniformed and overseas citizens to vote.

#### **2.1.2 Electronic Transmission Service**

In 1990 as part of Operation Desert Shield, the FVAP established the Electronic Transmission Service (ETS) that allowed voters to request and receive blank ballots from their state/jurisdiction via fax as well as to return the completed ballot to their state/jurisdiction via fax. The FVAP would receive the faxed voting material (absentee ballot requests, blank absentee ballots, completed absentee ballots, etc.) from the state/jurisdiction or voter. The FVAP would forward the voting material they receive to the appropriate state/jurisdiction or voter by fax. In October 2003, the FVAP expanded ETS to include a fax-to-email conversion capability. The fax-to-email conversion capability was added to support uniformed service members serving in Iraq and Afghanistan where faxing support was limited and email support was a viable alternative. A state/jurisdiction would have to consent to use the fax-to-email conversion capability as a method to distribute voting information between the state/jurisdiction and voter. For the fax-to-email conversion, a state/jurisdiction would fax voting material to the FVAP. The FVAP would convert the voting material received by fax into a read-only PDF file that would be emailed to the voter as an attachment. The voter would print the voting material including the blank absentee ballot, complete the absentee ballot, scan the completed absentee ballot into a PDF file, and email the completed absentee ballot to the FVAP as an attachment. The FVAP would then convert the voter’s PDF file into a fax for transmission to the voter’s State/jurisdiction. Today,

the FVAP also provides the capability to distribute voting material completely via email. Whether a completed absentee ballot is returned via a fax or email, the voter is instructed to always return the paper absentee ballot to their state/jurisdiction via conventional mail.

### **2.1.3 Voting over the Internet**

In 2000, FVAP initiated the Voting Over the Internet (VOI) project to determine if ballots could be reliably and securely cast over the Internet [15, 16]. The project was designed to mimic the established absentee voting process (see section 2.2 for a detailed description of the UOCAVA voting process). Voters who used the VOI system were required to obtain a Department of Defense (DoD) Public Key Infrastructure (PKI) digital certificate used for authentication and web browser plug-in software used to display and transmit ballots to servers administered by FVAP. A voter would use an electronic version of the FPCA to request an absentee ballot and digitally sign the FPCA using the DoD PKI digital certificate. When an electronic absentee ballot request was made, local election officials were notified of the request to be processed. Once a local election official approved the electronic absentee ballot request, a blank electronic ballot was placed on a FVAP server for retrieval. Using a web browser and plug-in, the blank electronic ballot would be retrieved, completed, encrypted, and the encrypted ballot digitally signed by the voter. The encrypted and signed ballots were placed on an FVAP server for retrieval by two local election officials. Note that the completed ballots stored on the FVAP servers were encrypted so that only the local election officials associated with the specific ballot could decrypt the ballots. Once decrypted, the electronic ballots were printed out so that they could be processed (tabulated) in the same way as mail-in absentee ballots. As part of the project, the voters who used the VOI system were allowed to cast traditional paper based ballots.

### **2.1.4 SERVE**

In 2002, the FVAP established the Secure Electronic Registration and Voting Experiment (SERVE) in response to Section 1604 of the National Defense Authorization Act for Fiscal Year 2002. Section 1604 directed the Secretary of Defense to carry out a demonstration project to enable uniformed service members to cast ballots through an electronic voting system by the 2004 general election. SERVE used a web-based architecture with servers hosted and administered by the FVAP. In general, SERVE provided the general capability to electronically identify and authenticate users (voters and local election officials) of the system using unique digital identities (enabled by digital signatures). Voters and local election officials would have to register to become users of SERVE and receive a digital identity. Voters could connect to servers hosted by FVAP to register to vote, request a blank electronic absentee ballot, and complete and return the absentee ballot electronically. Local election officials would connect to servers hosted by FVAP to receive information for voter registration, to receive requests for blank absentee ballots, to distribute electronic blank absentee ballots, to receive completed electronic ballots, and, optionally, ballot tabulation and reports.

In 2003, the FVAP assembled a Security Peer Review Group (SPRG) to review security aspects of the SERVE project. In January 2004, some of the SPRG members released a report highlighting concerns with the security of SERVE [14]. However, no official report was released from the complete SPRG membership. Later in 2004, the Secretary of Defense suspended the

SERVE project. The “Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005” called for the Secretary of Defense to wait until the EAC established electronic absentee voting guidelines before conducting another electronic voting demonstration project. In addition, HAVA calls for the EAC to consult with the Secretary of Defense to study best practices for facilitating voting by absent uniformed and overseas citizens. It should be noted that UOCAVA remote voting demonstration projects continue to be implemented by state and local election officials as well as public and private organizations. For example, Okaloosa County, Florida is conducting the Okaloosa Distance Balloting Project (ODBP) in partnership with the Operation BRAVO (Bring Remote Access to Voters Overseas) Foundation and the Center for Security and Assurance in Information Technology (C-SAIT) at Florida State University. ODBP placed voting kiosks in three overseas locations that allowed overseas voters to cast ballots in the November 2008 general election.

### **2.1.5 Interim Voting Assistance System**

In September 2004, the Department of Defense launched the Interim Voting Assistance System (IVAS 2004) to allow eligible absentee voters to request and receive absentee ballots over the Internet [16]. To participate in IVAS, users would have to be in the Defense Enrollment Eligibility Reporting System, a US citizen covered by UOCAVA, and already registered to vote in a participating jurisdiction. A voter would connect to the IVAS website running on a FVAP server using Secure Socket Layers (SSL) to request blank absentee ballot. Once a request was made, the appropriate local election official was notified of the request. After the local election official approved the request, the voter was notified via email that their ballot was ready. The voter would connect to the IVAS server via a secure connection in order to download and printout the blank absentee ballot. The voter would use traditional mail to send the completed printed ballot back to the local election official.

In September 2006, the Department of Defense launched the Integrated Voting Alternative Site (IVAS 2006), previously known as the Interim Voting Assistance System (IVAS), to assist UOCAVA voters [17]. IVAS consisted of two tools to request and receive blank absentee ballots– one using purely email messages, the other using a web server running the Secure Socket Layer (SSL) protocol. Both tools required a unique DoD identifier possessed by uniformed service members, their family members, and overseas DoD employees and contractors. The IVAS 2006 identifier requirement limited the UOCAVA population that could use IVAS 2006. Tool One used email messages to allow voters to request blank absentee ballots from their jurisdiction. Using the unique DoD identifier, the voter connected to Tool One over the Internet and logged on to get an electronic version of the Federal Post Card Application (FPCA) form to complete. Once the electronic FPCA was complete, the voter saved the completed electronic form on the local disk of the computer system used to connect to Tool One. The voter attached the completed electronic FPCA form as a PDF file to an email message sent to their local election official. It should be noted that the email sent to the local election official was not electronically/digitally signed by the voter.

The local election official received the blank absentee ballot request email and processed the request. If the absentee ballot request was approved, the local election official provided a blank absentee ballot via fax, email, or traditional mail based on the governing election law. After

receiving the ballot, the voter printed out the blank ballot and returned the completed ballot back to the local election official. Tool Two used a secure server to allow the request and delivery of the blank absentee ballots. Using the unique DoD identifier, the voter connected to the protected Tool Two server over the Internet, by the SSL protocol. The voter then completed an electronic version of the FPCA form that was saved to the Tool Two server for processing by a local election official. A local election official then connected to the Tool Two server over an Internet communication protected using the SSL protocol to download the blank absentee ballot request for processing. If the blank absentee ballot request was approved, the local election official posted a PDF file containing the blank absentee ballot. Then the voter securely reconnected to the Tool Two server to retrieve the blank absentee ballot and print the ballot. The voter then completed the blank absentee ballot and returned the completed ballot to the local election official. Neither Tool One nor Tool Two supported the return of completed absentee ballots electronically to the local election officials. Both tools only enabled voters to request and receive blank absentee ballots. It was up to the voter to return the completed ballots back to local election officials using mechanisms outside of IVAS 2006. These mechanisms included fax, e-mail, and traditional mail. In addition, it should be noted that both IVAS 2004 and 2006 did not provide the functionality for a user to register to vote in a jurisdiction. In IVAS 2004 and 2006, the user had to already be a registered voter in a given jurisdiction.

## **2.2 Current UOCAVA Voting Process**

The Department of Defense has implemented several different UOCAVA voting projects (ETS, VOI, SERVE, IVAS 2004, and IVAS 2006) over the last few years. Based on the workflows supported by the DoD UOCAVA projects, several general steps in the UOCAVA voting process can be identified. This section briefly describes the general steps of the UOCAVA voting process.

**Step 1:** The first general step in the UOCAVA voting process is to have the overseas citizen obtain a voter registration form in order to become a registered voter in the appropriate jurisdiction. Based on a jurisdiction's election laws, a voter could register to vote either before or while the voter is overseas or not in the jurisdiction physically. When a voter registers to vote while overseas, the voter would have to obtain the voter registration form via traditional mail or some electronic means such as fax, email, or website based on the jurisdiction's election laws. Once the voter receives the voter registration form, the voter will complete and return (via fax, email, website, or traditional mail) the form as prescribed by the jurisdiction. If a voter is currently registered to vote in the appropriate jurisdiction, the voter need not complete a voter registration form. The voter registration process for UOCAVA voters is facilitated by the use of the Federal Post Card Application (FPCA) either in paper or electronic forms based on a jurisdiction's election laws to register UOCAVA voters.

**Step 2:** The second general step in the UOCAVA voting process is for the voter to request a blank absentee ballot from the jurisdiction in which registered. Based on a jurisdiction's election law, a voter could request a blank absentee ballot either before or while the voter is overseas or not in the jurisdiction physically. When a voter requests a blank absentee ballot before going overseas or being physically away from the jurisdiction, a voter may be able to obtain the blank absentee ballot request form physically from a public location (such as the election office,

library, office of motor vehicles, etc.), have the form sent via traditional mail, electronically receive the form from a website or email from the jurisdiction, or be required to physically pickup the form from the jurisdiction's election office. If a voter requests a blank absentee ballot while overseas or not in the jurisdiction physically, the voter would have to obtain the blank absentee ballot request form via traditional mail or some electronic means such as fax, email, or website based on the jurisdiction's election laws. Once the voter receives the blank ballot request form, the voter will complete and return (via fax, email, website, or traditional mail) the form as prescribed by the jurisdiction. In addition to facilitating voter registration, the Federal Post Card Application (FPCA) can be used to request a blank absentee ballot either in paper or electronic form based on a jurisdiction's election laws. If a blank absentee ballot cannot be requested by a voter from the jurisdiction in time for a general election, the voter can complete the Federal Write-in Absentee Ballot (FWAB) for Federal offices (such as President/Vice President, U.S. Senator, and U.S. Representative).

**Step 3:** The third general step in the UOCAVA voting process is for local election officials to process the voter registration forms and blank absentee ballot requests. When a complete voter registration and blank absentee ballot request is received, the local election official will verify the voter's eligibility. If the voter is eligible to vote in the jurisdiction (including voter registration deadline date) and has met the blank absentee ballot request deadline date, the local election official will determine the proper ballot style for the voter and send the blank absentee ballot to the voter via traditional mail or some electronic means such as fax, email, or website based on the jurisdictions election laws.

**Step 4:** The fourth general step in the UOCAVA voting process is for the voter to receive (via fax, email, website, or traditional mail) the blank absentee ballot from their jurisdiction. When the blank absentee ballot is received, the voter completes the ballot either by printing and marking the ballot physically or electronically completing the ballot with the assistance of a web browser, kiosk, or other application software. Once the absentee ballot is completed, the voter may need to provide additional verification information such as a physical/digital signature or personal identification number (PIN) and date before returning the completed absentee ballot to the jurisdiction. After all jurisdictional requirements are completed, the voter will return the completed absentee ballot to the jurisdiction via traditional mail or some electronic means such as fax, email, or website based on the jurisdiction's election laws. If a blank absentee ballot is not received from the voter's jurisdiction, the voter can complete and return the Federal Write-in Absentee Ballot (FWAB) for Federal offices (such as President/Vice President, U.S. Senator, and U.S. Representative) to their jurisdiction.

**Step 5:** The fifth general step in the UOCAVA voting process is for the completed absentee ballots, including the Federal Write-in Absentee Ballots (FWABs), to be received for processing by the local election official. Once completed absentee ballots are received via traditional mail or via some electronic means such as fax, email, or website, the local election official will verify that the completed absentee ballots are valid. A local election official will verify that verification information such as physical/digital signatures and/or personal identification number (PIN) are valid, that the ballot was postmarked and/or received by the jurisdiction's deadline dates for absentee ballot return, and that the absentee ballot was completed as required by the jurisdiction (such as limited or no over voted races, use of only pencil or pen to mark choices, etc.). If the

absentee ballot verification information (signatures and/or PINs) is valid, the ballot is received before the absentee ballot return deadlines, and the ballot is completed as required by the jurisdiction, the local election official can include the absentee ballot as part of the election's tally based on the jurisdiction's election laws.

### **2.3 Difficulties in the Current UOCAVA Voting Process**

Although there is a general UOCAVA voting process currently used by overseas citizens, there are several difficulties in the process that need to be addressed.

One of the greatest difficulties is the time required to use traditional mail as a mechanism to distribute and receive election material (absentee ballot requests, blank absentee ballots, etc.). In general, the delivery times for postal and military mail to citizens overseas vary greatly depending where the citizen is located. It can take 5 to 10 days for most mail to be delivered to overseas citizens not in the military [25]; and 10 to 14 days for mail to be delivered to military personnel [24]. In addition, uniformed military and overseas citizens may not be at a given physical location for an extended period of time. Given that some jurisdictions finalize their ballots only 30-45 days before an election, using mail to distribute, receive and return election information can be difficult. In some cases the delivery times to distribute blank ballots and return them to local election officials could exceed the window of time between ballot printing and Election Day. This does not take into account the time required for election officials to process and handle blank ballots, or the time required for voters to fill out their ballots and drop them in the mail.

Another difficulty arises when voters use the emergency back-up mechanism for UOCAVA, the Federal Write-In Absentee Ballot (FWAB). First, the FWAB only covers Federal offices (e.g., President/Vice President, U.S. Senator, and U.S. Representative). In general, the FWAB does not allow a voter to vote on state or local questions, although some states will accept write-ins for state-wide offices on FWABs. Since the FWAB is a write-in ballot, the way the voter writes in a candidate's name on the ballot may impact the validity of the ballot based on a jurisdiction's election law. For example, mis-spelling a candidate's name (such as Bil for Bill) or not selecting the official candidate name (such as William, Bill, Billy, Will, Willy, etc.) could impact the ballot validity.

Finally, there are some difficulties common to absentee voting. One such difficulty is with signature verification. Signatures are the most common method for authenticating voters. However, verifying signatures is a difficult task. In order to verify a signature, a trusted sample signature must be on file with election officials. Comparing a received signature with a signature on file requires a great deal of training, although automated signature verification applications may make this task easier.

### 3 UOCAVA Voting Process

The basic five-step absentee and UOCAVA voting process outlined in Section 2.2 can be simplified and split into three stages: voter registration and ballot request, ballot delivery, and ballot return. This paper identifies and analyzes the use of several options for transmitting election materials for each of these stages. In this section we briefly describe the three stages of the overseas voting process. In each case we identify the types of information exchanged during that stage. The sensitivity of that information, combined with how it will be used during the election, determine the security needs of overseas voting systems implementing each stage, based on the potential impact of a violation of one or more of the security objectives. Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorizations of Federal Information and Information Systems*, [1] identifies and defines these objectives. Table 1, taken from FIPS 199, summarizes these definitions. Later sections of this paper will focus on how various transmission options could support each stage of the overseas voting process, and the threats to these types of systems.

Security Objective	Potential Impact		
	Low	Moderate	High
<b>Confidentiality</b> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
<b>Integrity</b> Guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
<b>Integrity</b> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Table 1: Potential Impact Definitions for Security Objectives [1]

### **3.1 Voter Registration and Ballot Request**

#### **Description:**

Voters register their names and legal voting residences with their local elections officials and request that blank ballots be delivered using postal mail, or some other electronic delivery method. This usually requires that voters provide some form of contact information, such as a mailing address, an e-mail address, or a fax number. The voter provides, or receives, and authenticator which can be used to verify that future correspondence. Typical authenticators include a voter's signature, a Personal Identification Number (PIN), or a digital signature and corresponding certificate.

#### **Information Types:**

Voter name, residency information, mailing address  
Voter authenticator (e.g. signature, PIN)  
Voter identifiers (e.g. social security, driver's license and/or passport numbers)

#### **Security Objectives:**

*Confidentiality*: High  
*Integrity*: Medium  
*Availability*: Medium

#### **Transmission Options:**

Postal mail, telephone, fax, e-mail, web-based.

#### **General Issues:**

Leaking sensitive personal information from voters.  
Available and integrity of voter registration database.

### **3.2 Ballot Delivery**

#### **Description:**

Election officials send a physical ballot, or a digital copy of a ballot, to all voters who have requested a ballot. Officials must determine the proper ballot style and send it to the voter using the contact information provided in the ballot request stage. In most cases, outgoing ballots contain tracking information that will be used by election officials when voted ballots are returned.

#### **Information Types:**

Candidate and Race information  
Possible ballot tracking identifier



### **Security Objectives:**

*Confidentiality*: Low

*Integrity*: High

*Availability*: High

### **Transmission Options:**

Postal mail, fax, e-mail, web-based.

### **General Issues:**

Voters must receive blank ballots in sufficient time to be able to return them to election officials before any deadlines.

Voters must receive the proper ballot styles, determined by their residency information.

Voters must receive blank ballots free from unauthorized modifications.

## **3.3 Ballot Return**

### **Description:**

Voters make their selections on their ballots and return the voted ballot to their local election officials. In nearly all cases, the voter will include an authenticator which can be used to verify the voter's identity. In many cases, the voted ballot includes tracking information that is used by election officials to verify that the returned ballot is the same one that was sent to the voter.

### **Information Types:**

Voter name, address(es)

Voter authenticator (e.g. signature, PIN)

Voter identifiers (e.g. social security, driver's license and/or passport numbers)

Ballot choices

### **Security Objectives:**

*Confidentiality*: High

*Integrity*: High

*Availability*: High

### **Transmission Options:**

Postal mail, telephone, fax, e-mail, web-based.

### **General Issues:**

Unauthorized individuals returning voted ballots.

Unauthorized individuals modifying voted ballots prior to ballot counting.

Improper disclosure of sensitive personal information from voters or voters' selections.

## **4 Description of Transmissions Options**

The purpose of this report is to identify options for distributing election materials to UOCAVA voters. This section will identify several different transmission options and provide brief descriptions for how these technologies and methods could be used to support overseas voting. The descriptions presented in Sections 4.2, 4.3, and 4.4 are merely examples of typical methods for employing the transmission options. This paper will outline threats to the types of systems described in this section, but other types of systems are possible.

### **4.1 Transmission Options**

This report considers the use of five different transmission options for the distribution and return of election materials: postal mail, telephone, fax, electronic mail, and web-based systems. This section briefly describes each of these transmission options.

#### **4.1.1 Postal Mail**

As indicated in Section 2.2, most communication between overseas voters and election officials takes place via United States postal mail, possibly in conjunction with the military postal service. In this case, a voter sends a form via first class mail to his or her local election official's office. Information, such as ballots, is returned by the official to the voter using the address on file, usually from the voter registration phase. The postal service is trusted to reliably transport these materials in a reasonable amount of time, without modifying or reading the contents of the packages. Undeliverable mail, such as when the destination address does not exist, is returned to the sender.

A thorough discussion of the deficiencies in such a system was included in Section 2.3.

#### **4.1.2 Telephone**

The Public Switched Telephone Network provides instant two-way communication between nearly any two telephones in the world. The telephone network is a global circuit-switched network consisting of a digital communications backbone with automated telephone exchanges routing calls to their destinations, and, in most cases, with an analog bridge from the backbone to end users' telephones.

Information can be communicated over the telephone network either verbally or by entering numbers on the touch-tone dial pad. In telephone voting systems, voters could communicate authentication information verbally or using the touch-tone dial pad. For instance, voters could enter a PIN on the dial pad, or answer questions verbally in a knowledge-based authentication system. In addition, it may be possible to use Caller ID information to partially authenticate voters.

#### **4.1.3 Fax**

Fax machines scan a document and transmit an encoded representation of it over the telephone network to another fax machine. The receiving fax machine can decode the information and

print a copy of the scanned document. Some fax machines create an analog representation of the document in a manner similar to analog television, while newer fax machines create a digital representation. The digital or analog representation is sent to the telephone network using analog signals.

Fax machines allow users to transmit written or printed information to another party. In many cases, they are used directly as an alternative to postal mail, allowing voters or election officials to fax election forms or ballots to the other party.

As is the case with telephone communication, telephone network operators are trusted to route faxes to the correct destination based on the number dialed, and not to modify or read faxes in progress.

#### **4.1.4 Electronic Mail**

Electronic mail, or e-mail, allows an individual to send text and/or files from one computer to another. This uses the Internet as a communications channel. Thus, the e-mail is transmitted from the sender's computer to his or her mail server (often operated by his or her Internet Service Provider, or ISP), and routed through a series of intermediate servers before being delivered to the recipient's mail server (often operated by an ISP, workplace or a commercial e-mail provider such as Gmail or Yahoo).

In the context of UOCAVA voting, in most cases, information transferred over e-mail would be sent with a form or ballot attached to the e-mail. In some cases it may be necessary for the sender to scan the form or ballot and save it in PDF [8] or other digital format in order to e-mail it.

Using standard e-mail, the recipient of a message does not receive any assurance of the identity of the sender, as it is easy to forge a return e-mail address. The sender may receive some assurance that the recipient received the e-mail. Many e-mail servers will send a warning to the senders of undeliverable e-mail. However, some e-mail servers, in order to limit unsolicited e-mails, do not sending these warnings.

E-mail can be encrypted. The current standard for e-mail encryption using Public Key Cryptography is the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol [22]. Most major e-mail clients include S/MIME functionality; however use of S/MIME encrypted e-mail is relatively rare. Use of S/MIME requires all users to have a public/private key pair and be part of a Public Key Infrastructure. Furthermore, commonly used web-based e-mail providers do not include S/MIME functionality. Because of the limited deployment and usage of S/MIME, this paper will assume e-mail communications are unencrypted unless otherwise noted.

#### **4.1.5 Web-Based**

It is also possible to use web sites to communicate between two parties. While both web sites and e-mail use the same communication channel, the Internet, the two options use different communication protocols. Also, the user experience in the case of a web site is vastly different

than that of e-mail. The interface can be customized, and the overall experience is more interactive.

A web-based UOCAVA voting system would include a web server operated by a local election official. That official could post information for all to see, such as blank registration forms, or blank ballots for each precinct. If this material is posted as a document, users could download files, print them, and return them to the official using some other form of communication. If the materials are posted as web forms, users could fill in the information on the web site and return it, in a manner similar to filling out billing information after purchasing something online.

Alternatively, the web site may grant different users access to different information. For instance, upon registration each voter would be given a username and password for the site. Upon logging on to the site, the voter would only have access to relevant information for him or her; for example, the voter would only see his or her ballot.

Properly developed and configured web sites can contain additional security protections not found in e-mail by using SSL (Secure Socket Layers) or TLS (Transport Layer Security) [4,7]. This would allow for encrypted communications between the web server and a voter to prevent eavesdropping. Digital certificates could be used to give voters assurance they are on the correct website. A more detailed discussion of security controls is presented below.

## **4.2 Options for Voter Registration and Ballot Request**

The previous section discussed five different transmission options for voting materials. The next three sections discuss how each of these options could be used to support the three stages of overseas voting. As previously noted, this section outlines typical election systems using the transmission options, but does not attempt to capture every possible variation.

The first stage of the UOCAVA voting process is the registration and ballot request stage. In this stage voters submit registration information confirming their identities and places of residence, and provide election officials with contact information. This section describes how election materials from this stage could be sent using postal mail, telephones, fax machines, electronic mail, and web-based systems.

### **4.2.1 Postal Mail**

As discussed in Section 2.2, all states accept the Federal Post Card Application (FPCA) to register military and civilian overseas citizens to vote and for requesting ballots. Voters obtain these forms from a variety of locations, including military voting assistance officers, embassies and consulates. Some web sites, such as the Overseas Vote Foundation [27], have posted copies of the form. Voters unable to find an FPCA may request one from military service departments or the State Department.

The FPCA asks each voter for his or her name, voting residence address, mailing address and additional contact information. This information is used to determine voter eligibility, contact voters if problems are discovered, and distribute voting materials, such as absentee ballots.

The FPCA is also used to establish a shared authenticator that election officials can use to verify future correspondence from the voter, in this case the voter's signature. To gain some level of assurance that the person who filled out the form is the individual claimed, the FPCA asks for the voter's military identification number or passport number. If a voter is unable to provide either of those, some states require a notary to sign the FPCA.

#### **4.2.2 Telephone**

The public telephone network could be used to exchange voter registration information. In this case voters could obtain the telephone number for their local election official and call to register to vote or request a ballot. Voters would speak to either an election official or an automated registration system, providing their name, voting residence address, and any contact information required, such as a telephone number or mailing address.

In order to authenticate the registration, each voter would need to provide sensitive, identifying information, such as a military identification number or passport number, which election officials could verify. Voters unable to provide the required identifying information would not be able to register over the phone. The election official and voter may use this time to establish a new shared authenticator for future correspondence, such as a PIN or a password. Alternatively, election officials and voters may continue to use the identifying information used to verify the voters' identities.

#### **4.2.3 Fax**

Several states allow voters to fax completed FPCAs to their local election officials. The procedures for marking and returning FPCAs are the same as for postal mail (see Section 4.2.1), except that the completed form is faxed to the local election official rather than mailed. The election official should have a dedicated fax line for receiving FPCAs, and this machine should be kept in a secure room.

#### **4.2.4 Electronic Mail**

Some states allow voters to e-mail completed FPCAs to their local election officials. In this case, each voter would have to obtain a paper copy of the FPCA, either by finding a physical copy of the form or printing an electronic version. The voter would sign the paper FPCA, and use a scanner to save it on his or her personal computer in a standard file format, such as the Portable Document Format (PDF). The resulting file could be sent as an attachment in an e-mail to a special e-mail address set up by election officials for registration and ballot requests.

In the typical case described above, a voter's signature is required in order to authenticate the source of the registration form. Election officials may be able to compare the signature on the form to voter registration information on file. Individual jurisdictions may determine that other information could be used to authenticate the voter's identity. This could include requesting confidential personally identifiable information that is verifiable by election officials. Digital signatures would provide an alternative method for authenticating voters. Voters with a

public/private key pair could digitally sign their registration forms, which could be verified by election officials upon receipt. Digital signatures would be nearly impossible to forge, and the process would not put sensitive personal information at risk of being intercepted. However, it would require a large-scale Public Key Infrastructure, which does not yet exist.

#### **4.2.5 Web-Based**

Voters could submit registration and ballot request information on an election official-operated web site. Voters could fill in registration information directly on the web site from an Internet browser, and submit the information without printing or scanning any forms. Web servers could implement cryptographic protocols (e.g. SSL/TLS) to protect information as it is transmitted to and from the voters.

Such a system could not rely on voter signatures for authentication purposes. Web-based registration would have to rely on other methods for voter authentication, such as those described in Section 4.2.4.

### **4.3 Options for Ballot Delivery**

The second stage of the UOCAVA voting process is the delivery of the ballots. In this stage, election officials send blank ballots to voters using the contact information submitted during the registration and ballot request phase. This section describes how blank ballots could be sent using postal mail, fax machines, electronic mail, and web-based systems. Telephone systems are not considered in this section, as any telephone voting system would also incorporate a mechanism for making ballot selections. Telephone voting systems will be discussed in the next section.

#### **4.3.1 Postal Mail**

Election officials begin to distribute paper ballots after they are printed. Upon receiving a ballot request from a voter, election officials look up the voter registration status of the voter and, once confirmed, determine the proper ballot style for that voter's precinct. The ballot is then sent to the mailing address indicated by the voter's ballot request. The complete package usually contains instructions, return envelopes and other items to facilitate the ballot marking and return process. These items will be discussed when postal mail ballot return is discussed.

To track the ballot request through the delivery process, officials indicate in their records that a particular ballot request has been accepted, processed and sent out. In some cases, identifying information is passed along with the ballot during the processing and delivery of the ballot. It is important to note that this information is not printed on the ballot, but rather it is a physically separate item that follows the ballot. For instance, it could be a barcode printed on the outside of an envelope containing the ballot.

#### **4.3.2 Telephone**

Ballot delivery via the public telephone network would only work in the context of a vote by phone system. This option will be discussed in the next section.

### 4.3.3 Fax

Blank paper ballots could be faxed to voters as an alternative to postal mail. Most of the process is similar to postal delivery of ballots. Upon receiving a ballot request from a voter, election officials look up the voter registration status of the voter and, once confirmed, determine the proper ballot style for that voter's precinct. Again, this ballot does not have any identifying marks that could tie a particular ballot back to a particular ballot request or voter. The ballot, along with ballot marking and return instructions, is faxed to the number listed on the voter's ballot request.

Detailed ballot tracking procedures are not necessarily required for delivery of blank ballots via fax. Election officials receive immediate notification that the ballot was successfully delivered to the voter's requested fax machine. However, tracking numbers may be used internally by election officials prior to faxing the ballot in order to track the ballot request and delivery process at the election offices. These numbers may also be used to identify that the same ballot faxed to a particular voter is the one returned by that voter.

### 4.3.4 Electronic Mail

As in the fax and postal mail options, upon receiving a ballot request, officials check the registration status of the voter and determine the appropriate ballot style. As in the processes described previously, this ballot should not contain any identifying marks that could be tied back to a particular voter. In this case, the ballot must be in a digital form, such as in a Portable Document Format (PDF) file [8]. Officials could have digital copies of all ballot forms, or they could construct digital ballots from paper ballots using a scanner.

The ballot is sent as an attachment from an election office computer in an e-mail to the voter-provided e-mail address. Marking and return instructions should accompany the ballot, usually as plain text in the e-mail message. As with any e-mail message, the message travels from the election office computer, to the office's Simple Mail Transfer Protocol (SMTP) server [9]. From there the server determines how to route the message to the recipient's e-mail address. In most cases the message will pass through a series of intermediate network devices before arriving at the recipient's e-mail server. The message will remain on the server until the recipient logs into their e-mail account. Depending on the e-mail protocol used by the recipient the message may be deleted off the server after being accessed by the voter. Generally, webmail providers retain copies of e-mails. Other providers, such as internet service providers, often provide POP3 service, which allows voters to download copies of e-mails, which are then promptly deleted from the server.

As previously mentioned, most e-mail servers will send error messages to the e-mail sender if the message is not deliverable (for instance, if the address does not exist, or if a server is malfunctioning). Therefore, election officials should, at a minimum, follow up on all returned e-mail messages with other forms of communication. For additional protection against undeliverable mail, officials could request return receipts from recipients. Such receipts are automatically generated by recipient computers and delivered to the sender when an e-mail message is actually read by the voter, as opposed to simply being delivered to the voter's e-mail server.

### **4.3.5 Web-Based**

Rather than sending digitized ballots to voters individually, jurisdictions could post ballots on a public web site and instruct voters to obtain their ballots via that site. When discussing web-based delivery of ballots in this paper, we will assume that ballots will be returned via postal mail, fax or electronic mail. Thus the posted ballots would be in a digital format, such as PDF, suitable for printing. We discuss web-based delivery and return of ballots in the next section.

For the purposes of this paper, we consider a web-based ballot distribution system that is connected to the voter registration database. After registering to vote via some other method, voters could navigate to the election web site. The site would prompt each voter for identifying information, such as his or her name, date of birth and a portion of his or her street address. This information is not used to strongly authenticate the identity of the voter, but rather to look up the voter in the registration database to determine the proper ballot style and present it to the voter. After downloading the ballot, the voter would mark the ballot on the computer or print it and mark it by hand. Ballots would be returned using postal mail, fax or electronic mail.

## **4.4 Options for Ballot Return**

The third stage of the UOCAVA voting process is ballot delivery stage. In this stage voters return voted ballots to their local election officials. This section describes how voted ballots could be sent using postal mail, telephones, fax machines, electronic mail, and web-based systems.

### **4.4.1 Postal Mail**

After receiving a physical or electronic blank ballot, a voter may, if necessary, print a paper ballot, and then make his or her selections on the ballot. In most jurisdictions, the voter is instructed to place the ballot in a privacy envelope, which may be a standard envelope or one provided by election officials. The privacy envelope is placed in an outer envelope, along with information used to authenticate the voter and the voted ballot (or this information is written on the outer envelope), creating a single package of voting material. This envelope may be placed in an additional return envelope, or placed directly in the mail. Upon delivery, outer envelopes are stored in a secure location until the election polls close and ballot tallying begins.

Multiple envelopes are used to protect voter privacy during the tabulation phase. Election officials open the outer envelope and separate identifying information from the privacy envelope prior to opening the privacy envelope and tallying the votes.

Many jurisdictions use ballot tracking procedures to follow individual ballots throughout the delivery, return and counting processes. Identification numbers and code, often in the form of barcodes, are included on individual ballots, privacy envelopes, outer envelopes, return envelopes, or some combination of those items. This provides some assurance that ballots are not lost during the tabulation process. Furthermore, election officials could use the information on the barcodes to verify that the same ballot that was sent to an individual voter was the one that



was returned by that voter, offering some protection against attacks. However, ballot tracking information could be used to violate voter privacy. In many cases, a large portion of the ballot tracking process is performed using automated systems or en masse, which provides some protection against malicious individuals attempting to use tracking information to determine how individuals voted.

#### **4.4.2 Telephone**

Telephone voting systems do not have distinct ballot distribution and return stages. Voters are provided with ballot questions and immediately given an opportunity to make selections. Voters would not have to wait for ballot materials to be distributed, but they would have to wait until they have received voting credentials and until the polls open on the telephone voting system.

In most cases, the telephone voting system would be a computer system with connections to several telephone lines. The computer system would automatically receive calls, provide voting instructions, authenticate voters and store cast ballots. Prior to opening the telephone polls, election officials would have to initialize the voting system with information about registered voters, authentication information, and ballot styles for all jurisdictions under their control. Voter information could be initialized using information from the registration and ballot request stage. For example, upon receiving a registration and ballot request, election officials would enter the voter's name and residency information in the voting system. This information would be used to identify the appropriate ballot style for a given voter. Election officials would also generate a random personal identification number (PIN) for the voter, and provide it to the voter and the voting system. The PIN would be used to authenticate the voter.

After the polls have been opened, voters could call the telephone voting system from their personal telephones, supply their name, residency information and PIN for authentication purpose, and cast a ballot by following the prompts on the phone.

Telephone voting systems are currently in use in the state of Vermont. However, the Vermont system is not used for remote voting, but rather to serve as an accessible voting station for visually impaired voters. Voters must still go to their local polling places to vote even if they will use the telephone voting system.

#### **4.4.3 Fax**

Fax machines could be used to transmit voted ballots to election officials. After receiving physical or electronic ballots, voters could make their selections on their ballots and print out paper copies, if necessary. Voters may also need to obtain one or more election forms, if they were not delivered via postal mail. These forms would have fields for the voter's name, residency information, signature, and other information needed by the election officials. Additionally, voters may be instructed to sign a form that includes information about privacy issues when using a fax machine to return a ballot. This package of materials, the voted ballot and accompanying forms, could then be faxed to an election official.

Upon receiving the faxed ballot and voter information, an election official would package this information together and store it in a secure location until the tabulation process begins. Unlike postal mail voting, there are no physical protections for maintaining vote secrecy. As part of the tabulation process, election officials would authenticate voters by comparing the voter's signature on the form with the signature on file from the registration process. In some cases, the selections on the faxed ballot are transferred to another ballot, such as an optical scan ballot.

#### **4.4.4 Electronic Mail**

Given the wide usage of e-mail in everyday communications, e-mail may be an attractive option for quickly returning electronic ballots to officials. In this paper, we consider a ballot return method using e-mail which closely follows the fax method. This method is already used by several states in the country.

The voting process would be very similar to the process described in Section 4.4.3 for ballots returned via fax. Voters would obtain and mark a paper ballot, and fill out accompanying voter forms for identification purposes. However, rather than faxing these materials to election officials, the voter would scan them on a computer, creating a digital copy of the ballot package, or use some other device capable of scanning and e-mailing attachments. Voters would have to save the scanned materials in a standard file format, such as PDF. The resulting file, or files, could be sent to election officials as attachments in an e-mail.

Upon receiving the ballot package, an election official would open the attachment and print a paper record of the ballot and accompanying voter forms. This package would be stored in a secure location, along with other paper ballots received via fax or postal mail. As was the case with fax return of ballots, there are limited procedural protections that could maintain voter privacy. Election officials charged with responding to e-mailed ballots would have access to voters' identities and ballot selections.

It may be possible to automate additional steps in this process using a computer. Depending on the format of the received ballots, a computer may be able to automatically tally votes as they are received via e-mail. They could also be used to assist election officials in authenticating received ballots. Some absentee ballot management systems even include signature verification functionality. In general, however, such systems are not considered in the threat analysis outlined in this paper.

#### **4.4.5 Web-Based**

In this paper, we consider web-based Internet delivery of ballots to be what many refer to as Internet voting. That is, web-based voting is a voting system in which voters make ballot selections and cast their votes on a web site operated by election officials. Like the telephone voting option described in Section 4.4.2, web-based Internet voting does not require a separate ballot delivery stage. Note that this paper considers web-based ballot delivery and web-based ballot return as two different types of voting systems. Section 4.3.5 covers only the distribution of blank ballots, and assumes some other method will be used to return voted ballots to election

officials. This section assumes the web site will allow voters to both view ballot contests and cast ballots with their selections.

Web-based Internet voting systems consist of an election web server connected to the Internet. The server would have similar functionality to the telephone system described in Section 4.4.2, in that it would authenticate voters, provide ballot contests, and record voters' selections. Voters would connect to the election web server from computers using a standard web browser.

Prior to opening the polls, election officials would have to initialize the voting system with information about registered voters, authentication information, and ballot styles for all jurisdictions under their control. For example, upon receiving a registration and ballot request, election officials would enter the voter's name and residency information in the voting system. This information would be used to identify the appropriate ballot style for a given voter.

The voting system would rely on the voter authenticator exchanged during the voter registration and ballot request stage. More traditional methods for absentee voting rely on voter signature verification for authentication purposes, which would not be possible in a web-based voting system. Typical authentication methods for web-based Internet voting include digital signatures, PINs and passwords. NIST SP 800-63, Electronic Authentication Guideline, [5] discusses several methods for remote authentication which could be used in an Internet voting system.

## 5 Threat Analysis Methodology

The remainder of this paper focuses on the security issues related to using these types of systems. Section 5 contains a threat analysis for each of the 14 systems considered in Section 4. This analysis was performed based on methodology provided in NIST SP 800-30, *Risk Management Guide for Information Technology Systems* [2], with some important modifications. The first step in the threat analysis is characterizing the election systems. Typically this is done with a particular system in mind, knowing what type of information will be handled, what procedures will be followed, and what equipment will be used. This report, however, looks at systems from a high level, where none of these items is known with any amount of specificity. The high level descriptions of transmission options for each stage of the voting process given in Section 4 characterize the systems analyzed in this report. As these characterizations are high level, the threat analysis must be performed at a correspondingly high level.

For each system, we identified methods (i.e., threats) for attackers to violate one of the major security goals of the election system: confidentiality, integrity and availability. We then consider the level of access to election systems, skills and resources that would be needed to carry out a threat. Based on that analysis, we identify a set of groups or individuals capable of carrying out a threat, and estimate the likelihood that election officials would be able to detect an attack from that group or individual. Finally, we propose security controls that could mitigate or eliminate the identified threat. The following subsections describe each of these stages in more detail.

### 5.1 Threats

Threats are events or circumstances that are potential violations of security. For each transmission option we list high-level threats that describe potential security problems. For example, a threat could involve compromising the privacy of votes, modifying cast ballots or making the voting system inaccessible to voters. Not all threats are caused by humans; natural disasters and equipment failures are potential threats, particularly to the availability of systems. However, this report focuses on threats, such as those from malicious individuals or groups, as these threats can attack any of the security objectives of a system in a variety of ways.

### 5.2 Threat Sources

Threat sources are groups or individuals that could feasibly attack a voting system. Some attacks on voting systems could be conducted by almost any dedicated individual, while others may require significant resources, knowledge or access to voting system equipment. Threat sources can be broken down into two classes: internal and external sources. Internal sources are individuals or groups with some level of authorized access to the voting system equipment or the supporting infrastructure (e.g. the communications network). External sources are individuals or groups that do not have any special level of authorized access to the voting system equipment or supporting infrastructure. This report considers the following examples of threat sources.

### Internal Threat Sources:

- **Legitimate Voters:** Legitimate voters have a limited level of access to voting system equipment. That is, each voter is allowed to submit registration information, obtain the proper ballot given their registration status, and cast a single ballot. Voters may, for example, attempt to use or expand their authorized level of access to damage the election system, change the results of the election, or harm the credibility of the election results.
- **Election Officials:** Election officials have a significant level of access to data on voting system equipment. They are users of the election system with access to voter and ballot information, but may not be authorized system administrators. However, while election officials may be restricted from certain administrative functions, such as software installation, they often have relatively unrestricted physical access to voting system equipment. Malicious election officials could use their privileged access to voting systems to exploit the system.
- **System Operators:** While election officials are users of an election system, system operators serve as administrators, ensuring that the systems function properly or seeing that vital operations are fulfilled. System operators may administer the election system directly, or they may administer the supporting infrastructure for the election. For example, postal mail employees, including mail carriers and sorters, would be system operators in elections which use the postal mail as a communications medium. Network technicians at major telephone companies or Internet Service Providers (ISPs) would be examples of system operators when the telephone network or the Internet is used. In all cases system operators have a privileged level of access to equipment that is vital to conducting the election.
- **Other insiders:** Other individuals or organizations may have privileged access to voting system equipment, either before, during or after an election is conducted. For example:
  - Voting System Manufacturers
  - Voting System Integrators
  - Support staff

### External Threat Sources

- **Hostile Individuals:** Individuals without special access privileges to the voting system may attempt to exploit vulnerabilities. In many cases, these individuals would be limited only by their technical knowledge and their ability to deceive individuals with privileged access to the voting system (e.g. social engineering). However, some types of attacks may require multiple attackers acting in unison or significant resources that one person cannot easily accumulate or control.
- **Hostile Organizations:** A hostile organization and a hostile individual differ in the amount of human and technical resources under their control. Hostile organizations would be able to recruit, hire, and train several individuals to participate in an attack. An organization would likely have more resources, both monetary and technical (e.g. computers, network bandwidth). Hostile organizations could take many forms. While their attacks motives may differ, the possible desired outcomes for attacks are likely the

same: controlling the result of the election, disrupting the voting process, or damaging the credibility of the election. Examples of hostile organizations include:

- *Hostile Civilian Organizations*
- *Foreign-Sponsored Organizations*
- *Terrorist Organizations*

### 5.3 Effort

Effort refers to the relative level of difficulty of performing a successful attack based on a threat. Each threat is classified into one of three levels:

- **Low:** An attack would require little or no resources or detailed knowledge of the system. *Example: Forcing a voter to vote a particular way in the presence of an attacker.*
- **Moderate:** An attack would require significant resources (or an ability to obtain such resources) or knowledge of the system. Inside attacks involving a small number of co-conspirators fall in this category. *Example: A Denial of Service (DoS) attack against election official computers and servers.*
- **High:** An attack would require extraordinary resources, knowledge of the system or access to the system. Inside attacks involving a large number of co-conspirators fall in this category. *Example: Replacing absentee ballots with forgeries during manual hand-counts.*

### 5.4 Detection

Organizations can recover from or mitigate attacks if they are detected. For each threat, this report estimates the relative level of difficulty of detecting whether a particular threat has been realized in an attack. In general, attacks are more severe when they go undetected. The threat matrix estimates the likelihood that an attack would be detected, and classifies it according to three levels:

- **High:** An attack would most likely be detected given proper monitoring. *Example: An attacker luring voters to an imposter election web site.*
- **Moderate:** An attack may be detectable, but could require a large amount of resources and time. Such attacks are unlikely to be detected during the election. *Example: A computer virus infecting personal computers.*
- **Low:** An attack is unlikely to be detected without extraordinary resources. *Example: Malicious code installed on election equipment by election insiders.*

### 5.5 Impact

The impact of an attack is its effect on violating the system's basic security objectives. The threat analysis includes *low*, *moderate* and *high* modifiers for each impact. The modifier indicates the likely severity of an attack from a given threat. Severe attacks must impact a significant number of votes or voters, or seriously damage the credibility of the election process. Descriptions of the security objectives and impact levels are described in Section 3, Table 1.

These goals are:

- **Confidentiality**
- **Integrity**
- **Availability**

## **5.6 Possible Controls**

Where possible, each threat is accompanied by possible mitigation techniques in the form of security controls from NIST SP 800-53 [3]. These controls are identified by the security control number. Section 7 of this report will discuss these controls in greater detail. In some cases, the systems targeted by an attack are outside the control of election officials. For instance, voters' personal computers are not administered by election officials, preventing officials from protecting those systems. Most threats to systems outside the control of officials do not have any suggested security controls.

## 6 Threat Analysis

The purpose of this report is to consider various technologies which could be used to improve the UOCAVA voting process and to identify high-level threats associated with each system. This section documents the threats identified using the methodology identified in Section 5. The threat analysis methodology used is a variation of the one outlined in NIST SP 800-30, *Risk Management Guide for Information Technology Systems* [2]. In particular, this report performs a threat analysis on each of the voting system transmission options identified in Section 4 for the three voting stages, Registration and Ballot Request, Ballot Delivery, and Ballot Return. Sections 4.2, 4.3, and 4.4 characterize how this report assumes each of these transmission options will be used in an election. In practice, many jurisdictions may use different procedures and technical controls while conducting elections. Specific threats and threat sources may differ slightly depending on the exact nature of how a particular transmission option is used.

Tables summarize the threats to each transmission option considered for the three stages. The first column of this table identifies the threat (see Section 5.1), while the second column identifies the individuals or groups capable of exercising that threat (see Section 5.2). The next three columns identify the level of effort required to exercise the threat (see Section 5.3), the relative probability that election officials would detect an attack (see Section 5.4), and the impact of the attack succeeding on the election (see Section 5.5). The final column identifies security controls that could mitigate the threat. Security controls are discussed in greater detail in Section 7 of this paper.

### 6.1 Registration and Ballot Request

This section documents threats to the transmission options for the Registration and Ballot Request stage, as described in Section 4.2.

#### 6.1.1 Postal Mail

The most widely used method for returning registration materials and requesting ballots is via postal or military mail. In this stage, voters send sensitive personal information to election officials to both identify themselves and to establish an address to send future correspondence, such as the blank ballot. One of the major concerns is that attackers could inject themselves in the communications path between the voter and the election official in order to collect personal information. The attacker could use this information to impersonate the voter, or possibly inflict financial damage on the voter (e.g. identity theft) depending on the type of information contained on the registration card.

Items in the mail are handled by a large number of people. In theory, any of the individuals charged with delivering a registration/request form could open the envelope to obtain personal information. However, this threat is substantially reduced by a variety of factors. Most postal carriers undergo some form of background check. Furthermore, it would be extremely difficult for a small number of malicious individuals to obtain a large amount of information. Most postal employees would only handle a small number of registration/request materials. In some cases it might be difficult to identify these materials from other pieces of mail without opening the



<i>Threat</i>	<i>Threat-Sources</i>	<i>Effort</i>	<i>Detection</i>	<i>Impact</i>	<i>Possible Controls</i>
Ineligible individual allowed to register to vote.	Hostile Individuals	Low	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5
Valid voter's ballot request information, such as address, is modified in transit.	Hostile Individuals Postal Workers System Operators Election Officials	Mod.	Low	Integrity-Mod.	MP-5, MP-5(1)
Registration/Request materials are accidentally lost or destroyed in transit.	Postal Workers	Low	High	Avail.-High	MP-5
Registration/Request materials are intentionally delayed or destroyed in transit by a malicious party.	Hostile individuals Hostile Organizations Postal workers	High	High	Avail.-High	MP-5
Sensitive personal information is viewed in transit.	Postal Workers	High	Low	Confid.-Mod.	MP-5
Sensitive personal information is improperly read after delivery.	Election Officials	Mod.	Mod.	Confid.-Mod	MP-1, MP-2, MP-4, PE-2, PE-3, PS-2, PS-3
Sensitive personal information is improperly modified after delivery.	Election Officials	Mod.	Mod.	Integrity-Mod.	MP-1, MP-2, MP-4, PE-2, PE-3, PS-2, PS-3

**Table 2: Threat Matrix for Postal Mail Registration and Ballot Request**

envelopes. Due to these factors, it is unlikely that a large scale loss of personal information could occur during transmission through the postal service.

One of the primary disadvantages of postal and military mail is the transmission time. Registration materials could be lost, destroyed, delayed or intercepted during transit from the voter to the election official. However, delays during registration and ballot request are not as damaging as at other points in the UOCAVA voting process. This stage of the process can occur well before an election, mitigating the damage caused by delays. With adequate lead time before an election, voters could also detect lost or destroyed registration materials, after noticing the absence of a response from election officials after mailing a form.

### 6.1.2 Telephone

Telephones could be used to transmit registration and ballot request information. One of the major functional differences compared to postal mail systems is that the standard form of authentication information, the voter's signature, would not be available for use. Voter authentication would have to be done using secret, and potentially sensitive, information identifying the voter. Depending on the type of information used, it may be easier for a group or individual to fraudulently register or request ballots for legitimate voters, as compared to processes that use both secret information and voter signatures.

As in the case with postal communication, there is a danger that transmitted personal information could be intercepted by malicious third parties. Information traveling over telephone lines could theoretically be intercepted by anyone with access to the telephone operator's equipment or physical lines. Many people, primarily telephone network employees, would have access to the equipment or lines. However, it would be extremely difficult for an individual or a group to successfully intercept personal information. The most likely scenario would be for an attacker to infiltrate the local central office near the election systems. Sabotaging the telephone network equipment, or jamming the telephone lines, would require a comparable amount of access to

<i>Threat</i>	<i>Threat-Sources</i>	<i>Effort</i>	<i>Detection</i>	<i>Impact</i>	<i>Possible Controls</i>
Ineligible individual allowed to register to vote.	Hostile Individuals	Low.	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5, IA-7
Election official offices have too few telephone lines to handle demand.	Telephone Operators System Operators	Low	High	Avail.-High	IR-4, IR-5
A denial of service attack, or other technical attack, jams telephone lines.	Telephone Operators Hostile Organizations	Mod.	High	Avail.-High Integrity-Mod.	IR-4, IR-5, CP-7, CP-8 SC-5, SC-8
Personal information is intercepted between the voter and election official.	Telephone Operators Hostile Organizations	High	Low	Confid.-Mod.	PE-4, SC-8, SC-9, SC-12, SC-13
Disgruntled election official fails to properly record registration information.	Election Official	Mod.	Low	Integrity-Mod.	PS-2, PS-3

**Table 3: Threat Matrix for Telephone Registration and Ballot Request**

network equipment, but would be significantly easier to conduct. Such an attack would prevent legitimate voters from sending their registration and ballot request information.

A recent development in the area of telephone communications is the adoption of voice-over-internet-protocol (VoIP) technology. Telephones using VoIP use the Internet to transmit calls, rather than the traditional telephone network, the Public Switched Telephone Network (PSTN). There are more opportunities for attackers to eavesdrop, disrupt and modify information on the Internet than the PSTN, particularly if individuals are using wireless access points to distribute their own Internet connection to VoIP devices.

Denial of service attacks are also a major concern. Individual jurisdictions would have a limited number of telephone lines available to them, and perhaps a more limited number of employees staffing them. An organization with significant resources could purchase enough telephone lines to prevent legitimate voters from speaking to election officials.

### 6.1.3 Fax

Fax machines would be able to transmit both secret information from the voter and the voter signature for authentication purposes. Fax machines use the telephone network to transmit information, so the same concerns about intercepted communications exist for registration via fax as for telephone calls. As previously noted, such attacks would be very difficult to carry out and require access to the telephone network infrastructure.

While a telephone call might be answered by an election official directly, or via an automated electronic process on a computer, fax machines would likely be left in a room at the election office receiving faxes throughout the day. In most cases the machines would be unattended. Received registration and ballot request forms could sit in the fax machine tray for several hours before being processed by an election official. This gives would-be attackers time to view sensitive personal information or destroy valid registration forms.

<i>Threat</i>	<i>Threat-Sources</i>	<i>Effort</i>	<i>Detection</i>	<i>Impact</i>	<i>Possible Controls</i>
Ineligible individual allowed to register to vote.	Hostile Individuals	Low.	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5, IA-7
Election official offices have too few fax machines and/or telephone lines to handle demand.	Telephone Operators System Operators	Low	High	Avail.-High	IR-4, IR-5
A denial of service attack, or other technical attack, jams telephone lines.	Telephone operators Hostile Organizations	Mod.	High	Avail.-High Integrity-Mod.	IR-4, IR-5, CP-7, CP-8, SC-5, SC-8
Personal information is intercepted between the voter and election official.	Telephone Operators Hostile Organizations	High	Low	Confid.-Mod.	PE-4, SC-8, SC-9, SC-12, SC-13
Disgruntled election official fails to properly handle faxed registration forms upon receipt..	Election Official	Mod.	Low	Integrity-Mod.	PS-2, PS-3
Sensitive personal information is improperly read from faxed registration forms prior to processing.	Election Officials Support Staff Hostile Individuals	Mod.	Mod.	Confid.-Mod	PE-2, PE-3, PE-5, PE-6, PS-2, PS-3
Sensitive personal information is improperly read from processed registration forms in storage.	Election Officials	Mod.	Mod.	Confid.-High	MP-1, MP-2, MP-4, PE-2, PE-3, PE-6, PS-2, PS-3

**Table 4: Threat Matrix for Fax Registration and Ballot Request**

Fax machines would not necessarily give voters instant notification that their registration and ballot request forms were received properly. Certain errors on the election official’s fax machines, such as low ink, would not be reported back to the voter automatically. Also, voters would not receive automatic notification if they filled out the forms incorrectly.

### 6.1.4 Electronic Mail

Electronic mail uses the Internet and a computer to transmit information. Voter authentication could be performed with some combination of secret personal information from the voter and a voter signature (the latter would require voters to print, sign and scan a physical paper ballot). There is potential for this information to be intercepted, and possibly modified, en route from the voter to the election official. E-mails travel through telecommunications lines, network equipment and e-mail servers before reaching the intended recipient. As e-mails travel unencrypted throughout the network, anyone with access to the infrastructure could read or even modify e-mail messages. In particular, e-mail servers often store messages for a short period of time before passing them on to the next server, or the intended recipient. System operators for these servers could possibly intercept registration e-mails.

E-mail does not provide any guarantee that the intended recipient will receive the message. The e-mail system relies on the Domain Name System (DNS) to route e-mails to the proper servers. An attack on DNS servers could route e-mails to an attacking party. This would not only result in voter disenfranchisement, but also the loss of sensitive voter information. This kind of attack would require very sophisticated attackers focusing their efforts on major e-mail service providers. There are no known reports of a similar attack being successfully conducted on e-mail or DNS servers. However, it is important to note that a recent vulnerability was discovered in DNS servers that could have been used to construct a similar attack [13]. DNS servers were

<i>Threat</i>	<i>Threat-Sources</i>	<i>Effort</i>	<i>Detection</i>	<i>Impact</i>	<i>Possible Controls</i>
Ineligible individual allowed to register to vote.	Hostile Individuals	Low.	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5, IA-7
Voter information from registration/request materials is read or modified on the e-mail servers of the voter or election official by authorized system administrators.	Network Operators	Low	Low	Integrity-Mod.	AC-2,AC-3, AC-5, AC-6, SC-9, SC-12, SC-13
Voter information from registration/request materials is read or modified on the e-mail servers of the voter or election official by unauthorized individuals.	Hostile Individuals Hostile Organizations	High	Mod.	Confid.-High Integrity-High	AC-2,AC-3, AC-5, AC-6, AC-12, SC-9, SC-12, SC-13
A denial of service attack against voter and/or election official e-mail servers overwhelms resources and prevents the transmission of registration/request materials.	Hostile Organizations	Low	High	Avail-High	IR-4, IR-5, CP-7, CP-8, SC-5, SC-7
Election official offices have too few resources (e.g. bandwidth, servers) to handle legitimate traffic.	Network Operators Election Officials	Low	High	Avail-High	IR-4, IR-5
Personal information is intercepted between the voter and election official on the Internet.	Hostile Organizations Network Operators	High	Low	Confid.-High	PE-4, SC-9, SC-12, SC-13
Malicious code (e.g. spyware) on the voter's computer transmits personal information from the registration/request materials to a third party.	Hostile Individual Hostile Organization	High	Mod.	Confid.-High	<i>Outside control of officials.</i>
Malicious code (e.g. a Trojan horse) on a voter's computer modifies or disrupts outgoing e-mails for with registration/request information.	Hostile Individual Hostile Organization	High	Mod.	Integrity-High	<i>Outside control of officials.</i>
Disgruntled election official fails to properly respond to e-mailed requests.	Election Official	Mod.	Low	Integrity-Mod.	PS-2, PS-3
Voters send registration/request materials to an incorrect e-mail address, resulting in the disenfranchisement and the loss of personal information.	Hostile Individual Hostile Organization	Low	High	Confid.-High Avail-Mod.	<i>Largely outside control of officials.</i>
An attack on the DNS system causes e-mails containing personal information to be sent to attackers.	Hostile Individual Hostile Organization	High	High	Confid.-High Avail-Mod.	SC-20, SC-21 <i>Note Largely outside control of officials.</i>

**Table 5: Threat Matrix for E-mail Registration and Ballot Request**

quickly patched before any significant attack took place, and changes to the DNS system are being implemented to prevent similar attacks in the future [12].

However, there are less sophisticated attacks that could disrupt the election process. A denial of service attack could flood election officials with a massive number of fraudulent e-mails. The number of e-mails could quickly overwhelm the election official's e-mail server, preventing legitimate registration forms from reaching election officials. Denial of service attacks are very difficult to defend against, although filtering incoming e-mails could provide some protection. However, the resources necessary to carry out the attack are readily available to malicious individuals or groups, using roughly the same technology as systems that send large amounts of unsolicited e-mail (i.e. spam). Depending on the e-mail server settings, voters may or may not be automatically informed that their registration materials were discarded.

Current e-mail-based attacks on banking sites point to phishing as a likely attack on e-mail-based registration systems. That is, an attacker would contact a large number of voters, claiming to be their local election official and attempting to convince them to reply with their voter registration information. While a relatively small number of voters may be tricked into supplying their information, the attack could be conducted on a large scale. It is relatively easy and cheap to contact a very large numbers of voters, some of whom would almost certainly be fooled.

Digital signatures would provide an alternative method for authenticating voters. Voters with a public/private key pair could digitally sign their registration form, which could be verified by election officials upon receipt. Digital signatures would be nearly impossible to forge, and the process would not put sensitive personal information at risk of being intercepted. However, it would require a large-scale, potentially nation-wide, Public Key Infrastructure, which does not yet exist.

### **6.1.5 Web-Based**

A web-based registration and ballot request system would perform voter authentication using secret personal information from the voter. However, unlike other systems, interception or modification in transit is not a significant threat. Any web-based system can and should incorporate encryption and integrity protection. All modern browsers ship with support for SSL/TLS [4,7], which is used extensively on e-commerce websites to provide such protections. Attackers may be able to intercept encrypted information in transit, but it is highly unlikely that they would be able to read or modify the protected information if web servers use properly configured implementations SSL/TLS.

While information in transit is secured, it would be possible to view voter information at the two end-points in the system: the voter's computer and the election web server. Malicious code, in the form of a computer virus or a Trojan horse, could record sensitive voter information and pass it to an attacker. Similarly, malicious individuals with access to the election web server could access sensitive voter information.

Attackers would be able to disrupt communications using denial of service attacks. A successful denial of service attack would overwhelm the election web server with traffic, preventing legitimate voters from sending registration and ballot request materials. It is very difficult to protect against denial of service attacks from an attacker with a large amount of resources. A successful denial of service attack generally requires access to a large number of computers with high-speed Internet connections. While an attacking organization may purchase these systems, it typically would use a Botnet. A Botnet is a collection of personal computers that have been infected with a virus that gives an attacker control of the computer. Control of Botnet-infected computers is sold on the black market, given nearly anyone with financial resources the technical resources to perform a denial of service attack.

<i>Threat</i>	<i>Threat-Sources</i>	<i>Effort</i>	<i>Detection</i>	<i>Impact</i>	<i>Possible Controls</i>
Ineligible individual allowed to register to vote.	Hostile Individuals	Low.	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5, IA-7
Voter information from registration/request materials is read or modified on thee election web server by authorized individuals.	Network Operators	Low	Low	Integrity-Mod.	AC-2,AC-3, AC-5, AC-6, SC-9, SC-12, SC-13
Voter information from registration/request materials is read or modified on thee election web server by unauthorized individuals.	Hostile Individuals Hostile Organizations	Mod.	Mod.	Confid.-High Integrity-High	AC-2,AC-3, AC-5, AC-6, AC-12, SC-9, SC-12, SC-13
A denial of service attack against the election web server overwhelms resources and prevents the transmission of registration/request materials.	Hostile Organizations	Mod.	High	Avail-High	IR-4, IR-5, CP-7, CP-8, SC-5
A denial of service attack against DNS servers disrupts access to the election web server	Hostile Organizations	High	High	Avail-High	<i>Outside control of officials.</i>
Election official offices have too few resources (e.g. bandwidth, servers) to handle legitimate traffic.	Network Operators Election Officials	Low	High	Avail-High	IR-4, IR-5
Sensitive personal information is intercepted between the voter and election official on the Internet.	Hostile Organizations Network Operators	High	Low	Confid.-High	PE-4, SC-6, SC-7, SC-12, SC-13
Malicious code (e.g. spyware) on the voter's computer transmits personal information from the registration/request materials to a third party.	Hostile Individual Hostile Organization	High	Mod.	Confid.-High	<i>Outside control of officials.</i>
Malicious code (e.g. a Trojan horse) on a voter's computer modifies or disrupts communication with the election web server.	Hostile Individual Hostile Organization	High	Mod.	Integrity-High Avail.-Mod.	<i>Outside control of officials.</i>
Defects in the election web server software causes voter information to be recorded incorrectly.	System Manufacturers	Mod.	Low	Integrity-High	SI-2, CM-2, CM-3, CM-5
Malicious code is inserted into the election web server which causes voter information to be recorded incorrectly.	Hostile Individual Hostile Organization	High	Mod.	Integrity-High	IA-2, AC-3, CM-5, MA-2, MA-3, MA-5, SI-3, SI-4, SI-7, PE-2, PE-3, PS-2, PS-3
Voters submit registration request materials to an incorrect web site (e.g., through phishing).	Hostile Individual Hostile Organization	Mod.	High	Confid.-Mod. Avail.-Mod.	<i>Largely outside control of officials.</i>
An attack on the DNS system forwards voters to an incorrect web site..	Hostile Individual Hostile Organization	High	High	Confid.-High Avail.-Mod.	SC-20, SC-21 <i>Note Largely outside control of officials.</i>

**Table 6: Threat Matrix for Web-Based Registration and Ballot Request**

However, the most likely threat for web-based registration processes comes from attackers that lure voters to fake websites posing at legitimate sites operated by election officials. This could be done via sophisticated technical attacks, or simple social engineering attacks. Internet web sites rely on DNS [11] to route traffic to the correct web server using a human-readable address. An attacker could trick one or more DNS servers into thinking that a fraudulent web server is a proper election web server. Voters attempting to navigate to their local election official's website could unknowingly navigate to a fake website, and supply attackers with sensitive personal information. Alternatively, an attacker could lure voters to a fake site by e-mailing them a link to a fraudulent web site. This is a common attack on Internet banking users.

Digital signatures would provide an alternative method for authenticating voters. Voters with a public/private key pair could digitally sign their registration form, which could be verified by election officials upon receipt. Digital signatures would be nearly impossible to forge, and the process would not put sensitive personal information at risk of being intercepted. However, it would require a large-scale, potentially nation-wide, Public Key Infrastructure, which does not yet exist.

## **6.2 *Ballot Distribution***

The section documents threats to the transmission options for the Ballot Distribution stage. This section discusses threats to systems which use postal mail, fax machines, electronic mail, and web sites to distribute blank ballots to registered UOCAVA voters. The systems analyzed in this section are discussed in Section 4.3. Note that telephone systems are not considered in this section. Telephone voting systems provide voters with ballot questions and allow voters to select their votes. Therefore, telephone voting systems are a type of ballot return system, and are discussed in Section 6.3.2.

### **6.2.1 *Postal Mail***

It is important for blank ballots to reach individual voters quickly and without modification. Postal mail is the slowest communications method considered in this paper. One of the greatest threats to postal mail delivery of ballots is not necessarily a malicious attack; it is that the unexpected delays in the postal mail system would cause ballots to be delivered too late to voters. Given transit times between many overseas locations and local election offices, it is unlikely that it would be possible to successfully recover from such delays.

Large scale malicious attacks are difficult to conduct on postal mail delivery of ballots. The only individuals capable of preventing the proper distribution of blank ballots to a large number of voters are election officials charged with operating the system. Smaller scale attacks on individual voters, or on a small number of voters are also possible, but their effect would be limited. Hostile individuals could steal blank ballots directly out of a voter's mailbox or place of residence, but this would not pose a major threat to the election as a whole.

Threat	Threat-Sources	Effort	Detection	Impact	Possible Controls
Individual delays or disrupts the process of preparing and/or mailing ballots.	System Operators Election Officials	Mod.	High	Avail.-High	PE-2, PE-3, PS-2, PS-3
Election official incorrectly indicates a voter is sent a ballot.	System Operators Election Officials	Mod.	Mod.	Avail.-Mod.	AC-2, AC-3, AC-5, AC-6, PS-2, PS-3
Election official sends a voter the wrong ballot.	Election Officials	Mod.	High	Avail.-Mod.	AC-2, AC-3, AC-5, AC-6, PS-2, PS-3
Normal mail service fluctuations cause some ballots to be delivered late, or not at all.	Postal Workers	Low	High	Avail.-Mod.	MP-5, IR-4, IR-5
An attack disrupts mail service, causing some ballots to be delivered late, or not at all.	Postal Workers Hostile Individuals	Low	High	Avail.-Mod.	MP-5, IR-4, IR-5
Individual intercepts mailed ballots prior to being picked up by the intended recipient.	Hostile Individuals	Low	High	Avail.-Low	MP-5
Individual modifies electronic ballot file prior to ballot printing.	System Operators Election Officials	High	High	Integrity-Mod	AC-2, AC-3, AC-5, AC-6, PE-2, PE-3, PS-2, PS-3,
Individual modifies paper ballots.	Election Officials	Mod.	High	Integrity-Mod	PE-2, PE-3, PS-2, PS-3, MP-1, MP-2, MP-4
Blank ballots are printed too late to reach voters on time.	System Operators Election Officials	Mod.	High	Avail.-High	IR-4, IR-5

**Table 7: Threat Matrix for Postal Mail Ballot Delivery**

## 6.2.2 Fax

Faxed distribution of blank ballots would not be subject to the same problems as the postal mail with delivery times. Faxed ballots would reach their destination nearly instantaneously. While it may be possible for an individual to eavesdrop on the faxed communications, this would only be a concern if blank ballots are accompanied by sensitive personal information about the voter.

Voters would not be able to predict the exact delivery time of their blank ballots. In many cases, ballots may be sent to a public fax machine, perhaps one shared by multiple employees at a

Threat	Threat-Sources	Effort	Detection	Impact	Possible Controls
Individual delays or disrupts the process of preparing and/or faxing ballots.	System Operators Election Officials	Mod.	High	Avail.-High	PE-2, PE-3, PS-2, PS-3
Election official incorrectly indicates a voter is sent a ballot.	System Operators Election Officials	Mod.	Mod.	Avail.-Mod.	AC-2, AC-3, AC-5, AC-6, PS-2, PS-3
Election official sends a voter the wrong ballot.	Election Officials	Mod.	High	Avail.-Mod.	AC-2, AC-3, AC-5, AC-6, PS-2, PS-3
An unauthorized individual takes a faxed ballot intended for a different voter.	Hostile Individuals	Low	Mod.	Avail.-Low	<i>Outside control of officials.</i>
A denial of service attack, or other technical attack, prevents outgoing faxes.	Telephone Operators Hostile Organizations	High	High	Avail.-Mod	IR-4, IR-5, SC-5, CP-7, CP-8, SC-13, SC-14
An individual modifies the paper ballots used by election officials prior to faxing a copy to a voter.	System Operators Election Officials	High	High	Integrity-Mod	PE-2, PE-3, PS-2, PS-3, MP-1, MP-2, MP-4

**Table 8: Threat Matrix for Fax Ballot Delivery**



workplace. Blank ballots may remain in the fax machine for an extended period of time before being noticed by the intended recipient. This would provide would-be attackers with ample opportunities to intercept the ballot before it reaches the intended recipient. While it would be very difficult for a single individual to intercept a large number of blank ballots, there are some situations where this might be possible. A single individual at a military base may collect and distribute faxes for a large number of soldiers stationed at the base.

Faxed ballots have little integrity protection in transit. However, it is quite difficult to modify faxes in transit, so this is not a significant threat. A more serious threat is that ballots could be modified prior to being faxed by malicious election employees, or after being sent to the recipient's fax machine. Voters may be able to detect changes to the ballot if certain ballot questions have been left off or modified.

### **6.2.3 Electronic Mail**

E-mailed ballots would not be subject to the same problems as the postal mail with delivery times. Like faxed ballots, e-mailed ballots would reach their destination nearly instantaneously. Eavesdropping is a potential threat whenever Internet communications are involved, and particularly with e-mailed communications, which are sent unencrypted. However, as ballot contest information need not be secret, eavesdropping is only a significant threat if ballots are accompanied by sensitive personal information about the voter.

E-mails are significantly easier to intercept and modify in transit than other forms of communication. E-mails travel through telecommunications lines, network equipment and e-mail servers before reaching the intended recipient. Anyone with access to the infrastructure could read or even modify e-mail messages. In particular, e-mail servers often store messages for a short period of time before passing them on to the next server, or the intended recipient. System operators for these servers would be in a good position to intercept or modify e-mailed ballots. Voters may be able to detect any changes made to the blank ballot. In addition, certain technical measures could be taken to assist voters in identifying improperly modified ballots.

Denial of service attacks are possible against election official e-mail servers, but very difficult to conduct. While it is comparatively easy to prevent an individual or organization from receiving an e-mail, it is much more difficult to stop a message from being sent. While blank ballot delivery is time-sensitive, the acceptable time frame window is several days. This would likely provide election officials with a sufficient amount of time to recover from any denial of service attack and distribute blank ballots on time.

Threat	Threat-Sources	Effort	Detection	Impact	Possible Controls
Individual delays or disrupts the process of preparing and/or e-mailing ballots.	System Operators Election Officials	Mod.	High	Avail.-High	PE-2, PE-3, PS-2, PS-3
Election official incorrectly indicates a voter is sent a ballot.	System Operator Election Official	Mod.	Mod.	Integrity-Mod.	AC-2, AC-3, AC-5, AC-6, PS-2, PS-3
Election official sends a voter the wrong ballot.	Election Official	Mod.	High	Integrity-Mod.	AC-2, AC-3, AC-5, AC-6, PS-2, PS-3
An unauthorized individual gains access to the voter's computer and/or e-mail accounts and accesses the blank ballot.	Hostile Individual	Mod.	Low	Confid.-Low	<i>Outside control of officials.</i>
Ballot files are modified on the e-mail servers of the voter or election official by authorized system administrators.	System Operators Election Officials	Mod.	Low	Integrity-Mod.	PS-2, PS-3, AC-3, AC-5, AC-6, SC-8
Ballot files are modified on the e-mail servers of the voter or election official by unauthorized individuals.	Hostile Individual Hostile Organization	High	Low	Integrity-Mod.	AC-3, AC-5, AC-6, IR-4, IR-5, SC-7, SC-8, SI-5
A denial of service attack against voter and/or election official e-mail servers overwhelms resources and prevents the transmission of blank ballots.	Hostile Organization Network Operators	High	High	Avail.-High	IR-4, IR-5, SC-5, CP7, CP-8, SC-14
Election official offices have too few resources (e.g. bandwidth, servers) to handle legitimate traffic.	Network Operators Election Officials	Low	High	Avail.-High	IR-4, IR-5
A voter receives a spoofed e-mail with an improper blank ballot or instructions, and assumes it is proper.	Hostile Individual Hostile Organization	Low	High	Integrity-High	SC-8, SC-13, SC-14
Malicious code (e.g. a Trojan horse) on a voter's computer modifies the received ballot or prevents the proper delivery of the ballot.	Hostile Individual Hostile Organization	High	Mod.	Integrity-High Avail.-High	<i>Outside control of officials.</i>
An attack on the DNS system prevents ballots from reaching their intended recipients.	Hostile Individual Hostile Organization	Mod.	High	Avail.-Mod.	IR-4, IR-5, SC-20, SC-21

Table 9: Threat Matrix for E-mail Ballot Delivery

## 6.2.4 Web-Based

Web-based communication can be easily protected using properly configured SSL/TLS, virtually eliminating the threat of eavesdropping or ballot modification in transit. Some attacks could take place at the endpoints: on the election web server and on voters' computers. A malicious election official could load improper ballots on the web site, although this would likely be quickly detected and resolved. Smaller scale attacks could take place on voters' computers. A hostile individual with access to a voter's computer could modify already downloaded ballots.

A significant threat to web-based ballot distribution is that attackers could lure voters to fake web sites posing as legitimate sites operated by election officials. This could be done via sophisticated technical attacks, or simple social engineering attacks. Internet web sites rely on DNS to route traffic to the correct web server using a human-readable address. An attacker could trick one or more DNS servers into thinking that a fraudulent web server is a proper election web server. Voters attempting to navigate to their local election official's website could unknowingly find themselves on a fake website. Voters may provide their voter credentials on this web site, potentially allowing the attacker to impersonate them in future transactions. Voters

Threat	Threat-Sources	Effort	Detection	Impact	Possible Controls
Individual delays or disrupts the process of preparing ballots or uploading them to the election web server.	System operators Election officials	Mod.	High	Avail.-Mod.	PE-2, PE-3, PS-2, PS-3
An unauthorized individual gains access to the voter's computer and accesses an already-downloaded blank ballot.	Hostile Individuals	Mod.	Low	Confid.-Low	<i>Outside control of officials.</i>
An unauthorized individual downloads a blank ballot intended for a different voter by gaining improper access to the election web server.	Hostile Individuals	Mod.	Low	Integrity- Mod. Avail.-Mod.	AC-2, AC-3, IA-2, SC-7, SI-4
Blank ballots are modified on the election web servers by authorized system administrators.	System operators Election officials	Mod.	Low	Integrity-Mod.	PE-2, PE-3, PE-6, PS-2, PS-3, AU-2, AU-3, AU-4, AU-6, AU-7, AU-8, AU-9, AU-10, AC-2, AC-3, AC-5, AC-6, SC-8, SC-13
Blank ballots are modified on the election web servers by unauthorized individuals with physical access to the server.	Hostile Individuals	High	Mod.	Integrity-Mod.	AC-2, AC-3, IA-2, PE-2, PE-3, PE-5, PE-6, PS-2, PS-3, SC-8, SC-13
Attackers remotely access election web servers and modify blank ballots.	Hostile Individuals	High	Mod.	Integrity-Mod.	AC-2, AC-3, IA-2, SC-7, SI-4
A denial of service attack against voter and/or election official e-mail servers overwhelms resources and prevents the transmission of blank ballots.	Hostile Organizations	Mod.	High	Avail-High	IR-4, IR-5, CP-7, CP-8, SC-5
Election official offices have too few resources (e.g. bandwidth, servers) to handle legitimate traffic.	Network Operators Election Officials	Low	High	Avail-Mod.	IR-4, IR-5
A voter is tricked into going to a spoofed site to download a fake ballot.	Hostile Individual Hostile Organization	Low	High	Integrity-High	<i>Largely outside control of officials.</i>
An attack on the DNS system forwards voters to an incorrect website.	Hostile Organizations	High	High	Avail-High	SC-20, SC-21 <i>Note Largely outside control of officials.</i>
Malicious code (e.g. a Trojan horse) on a voter's computer modifies the received ballot or prevents the proper delivery of the ballot.	Hostile Individual Hostile Organization	High	Mod.	Integrity-High Avail.-High	<i>Outside control of officials.</i>

**Table 10: Threat Matrix for Web-Based Ballot Delivery**

may also download improper ballots that, if marked and returned, would have to be thrown out by election officials. Alternatively, an attacker could lure voters to a fake site by e-mailing them a link to a fraudulent web site. This is a common attack on Internet banking users.

Denial of service attacks are a significant threat to any web-based ballot distribution mechanism. A successful denial of service attack would overwhelm the election web server with traffic, preventing legitimate voters from obtaining blank ballots. As previously noted, it is very difficult to protect against denial of service attacks from an attacker with a large amount of resources. A successful denial of service attack generally requires access to a large number of computers with high-speed Internet connections, but such resources could be easily obtained by buying time on a Botnet.

Malicious code on voters’ computers could prevent them from successfully downloading a ballot. A computer virus could prevent a voter from reaching the election web site, or it could even redirect the voter to an attacker’s fraudulent web site. Voters who do not detect the fraudulent site might enter their voter credentials on the site, potentially allowing the attacker to impersonate those voters in future transactions.

### 6.3 Ballot Return

The section documents threats to the transmission options for the return of ballots. This section discusses threats to systems which use postal mail, telephones, fax machines, electronic mail, and web sites to allow voters to submit votes to their jurisdictions. The systems analyzed in this section are discussed in Section 4.4.

#### 6.3.1 Postal Mail

Returning voted ballots is a very time-sensitive task. Many voters do not receive blank ballots until very close to the Election Day, which does not give them a lot of time to vote and return the ballot. Most states have deadlines for when absentee ballots must be postmarked and delivered to election offices. Malicious postal workers may be able to selectively identify absentee ballots in the mail, and disrupt delivery. However, typically a single employee would not encounter enough absentee ballots to pose a significant threat to the election outcome, except, for example, on a military base where a single soldier handles all outgoing mail. Hostile organizations may be able to attack sorting facilities or transports. Such attacks would be very dangerous and difficult to conduct, and the likely number of ballots affected is small. However, normal fluctuations in delivery times could affect a large number of voters, delaying their ballots long enough to cause them to miss deadlines imposed by states.

Threat	Threat-Sources	Effort	Detection	Impact	Possible Controls
Impersonation of registered voter (e.g., forged signature).	Hostile Individuals	Mod.	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5,
Voter coerced into voting a particular way.	Hostile Individuals	Low	Mod.	Confid.-Mod.	<i>Outside control of officials.</i>
Normal mail service fluctuations cause some ballots to be returned late, or not at all.	Postal workers	Low	High	Avail.-Mod.	MP-5
An attack disrupts mail service, causing some ballots to be returned late, or not at all.	Postal workers Hostile Organizations	High	High	Avail.-Mod.	MP-5
A large-scale attack on a postal mail hub disrupts mail delivery for a large group of voters.	Hostile Organizations	High	High	Avail.-High.	MP-5, IR-4, IR-5
Sensitive voter information is intercepted from the ballot while it is in the mail.	Postal workers System operators Election officials	Mod.	Low	Confid.-Low	MP-5
Marked ballots are modified or destroyed at the election office.	System operators Election officials	High	Mod.	Integrity-Mod.	MP-1, MP-2 (1), MP-4, PE-2, PE-3 (1), PS-2, PS-3
Marked ballots are viewed by unauthorized personnel, resulting in loss of voter privacy.	System operators Election officials Postal worker	High	Low	Confid.-Mod.	MP-1, MP-2 (1), MP-4, PE-2, PE-3 (1), PS-2, PS-3
Election officials are flooded with a large number of illegitimate ballots.	Hostile Organizations	Mod.	High	Avail.-Mod. Integrity-Mod.	MP-2

Table 11: Threat Matrix for Postal Mail Ballot Return

Confidentiality is important during the ballot return stage of the voting process. At a minimum, a ballot will show a voter’s selections on the ballot questions. In some cases, the ballot may be accompanied by sensitive personal information about the voter. While postal employees and hostile organizations may be able to intercept and read a small number of ballots, the overall effect on the election would be quite small. It is difficult to imagine a large scale loss of personal information during transmission through the postal service.

Voted ballots are at higher risk before and after transmission through the mail. Hostile individuals could steal a ballot from a legitimate voter, forge the voter’s signature and return the voted ballot to the election official. Alternatively, a hostile individual could coerce a voter into voting for a particular candidate. In either case, a single hostile individual or organization would be limited in the number of votes they could steal or unduly influence. There is far more potential to influence or damage an election at the election official’s offices. There, a large number of voted ballots would be collected and stored for several days or weeks. Hostile individuals with physical access to these ballots could violate voter secrecy, modify ballots, or destroy ballots. Tight physical access controls could reduce, but not eliminate, this threat.

### 6.3.2 Telephone

Telephone voting would virtually eliminate delays caused by ballot distribution and return. The voter would be given a set of ballot options and immediately be allowed to select his or her

Threat	Threat-Sources	Effort	Detection	Impact	Possible Controls
Impersonation of registered voter (e.g. stolen PIN).	Hostile Individuals	Mod.	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5, IA-7
Voter coerced into voting a particular way.	Hostile Individuals Hostile Organizations	Low	Mod	Confid.-Mod	<i>Outside control of officials.</i>
Election official offices have too few telephone lines to handle demand.	Telephone Operators System Operators	Low	High	Avail.-High	IR-4, IR-5
A denial of service attack against the election official office jams telephone lines.	Telephone operators Hostile Organizations	Mod.	High	Avail.-High	IR-4, IR-5, CP-7, CP-8, SC-5
Sensitive personal information or ballot selections are intercepted en route.	Telephone Operators Hostile Organizations	High	Low	Confid.-Mod.	PE-4, SC-8, SC-9, SC-12, SC-13
Voter ballot selections are viewed on the server by individuals with authorized access to the election system, resulting in loss of voter privacy.	Election Official System Operators	Mod.	Low	Confid.-High.	PE-2, PE-3, PE-6, PS-2, PS-3, AU-2, AU-3, AU-4, AU-6, AU-7, AU-8, AU-9, AU-10, AC-2, AC-3, AC-5, AC-6
Voter ballot selections are viewed on the server by unauthorized personnel, resulting in loss of voter privacy.	Hostile Individuals	High	Mod.	Confid.-High	AC-2, AC-3, IA-2, PE-2, PE-3, PE-5, PE-6, PS-2, PS-3
Defects in the voting system server software cause votes to be recorded incorrectly	System Manufacturers	Mod.	Low	Integrity-High	SI-2, CM-2, CM-3, CM-5
Malicious code is inserted into the voting system server software which causes votes to be recorded incorrectly	Election Official System Operators	Mod.	Low	Integrity-High	IA-2, AC-3, CM-5, MA-2, MA-3, MA-5, SI-3, SI-4, SI-7, PE-2, PE-3, PS-2, PS-3
An attacker tricks voters into calling the wrong phone number to vote.	Hostile Individual Hostile Organization	Low	High	Integrity-High	<i>Largely outside control of officials.</i>

Table 12: Threat Matrix for Telephone Ballot Return

choices. As noted in Section 6.1.2, it may be possible for hostile individuals with access to the telephone network infrastructure to eavesdrop on or disrupt these telephone calls. The threat is increased in the case of cellular phone communications. In general, however, a successful large-scale attack would be needed to target the communications equipment close to the election office housing the telecommunications equipment. This would substantially reduce the number of individuals capable of conducting an attack.

Sabotaging the telephone network equipment, or jamming the telephone lines, would require a comparable amount of access to network equipment, but would be significantly easier to conduct, particularly in the case of jamming cellular phone communications. Such an attack would prevent legitimate voters from accessing the equipment necessary to cast a ballot. Attackers could also conduct a denial of service attack on the telephone voting system by continuously calling and tying up communications lines. This would also prevent legitimate voters from casting a ballot.

Most telephone systems could feature an automated calling center capable of interacting with the voter similar to those used by many businesses. Election officials would not need to physically handle voted ballots, but would have access to the information stored on the server. While access control mechanisms could restrict access to this information, any hostile individual capable of bypassing these controls could change or delete a large number of ballots. A sophisticated attacker may be able to make these changes without leaving any evidence in, for example, the system event log.

Automated telephone voting is a form of electronic voting. The computer system running the automated calling center would have to be trusted to accurately record voters' selections. Defects in the voting system software, or malicious code installed on the voting system by hostile individuals, could cause votes to be recorded improperly, or could modify votes at a later time.

As noted in Section 6.1.2, some individuals and organizations are using Voice-over-Internet-Protocol (VoIP) telephones, which transmit information over the Internet instead of the public telephone network. Use of the Internet to transmit their ballot selections and choices would substantially increase the risk of eavesdropping and modification attacks in-transit. Such systems would be subject to many of the risks associated with e-mail and web-based Internet voting.

### **6.3.3 Fax**

Faxed ballot return is an alternative to mailing ballots. A fax-based system for returning ballots would not experience problems with delays. However, certain election officials would have the necessary level of access to compromise voter secrecy, and potentially to modify votes. Faxed ballots could remain in the fax machine for some period of time before being placed in a secure ballot box. Individuals with access to the fax machine or the ballot box would be in a position to violate voter privacy by accessing these ballots. Also they might be able to replace the faxed ballots with other ballots containing different votes.

Threat	Threat-Sources	Effort	Detection	Impact	Possible Controls
Impersonation of registered voter (e.g. forged signature).	Hostile Individuals	Mod.	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5, IA-7
Voter coerced into voting a particular way.	Hostile Individuals Hostile Organizations	Low	Mod	Confid.-Mod	<i>Outside control of officials.</i>
Election official offices have too few fax machines and/or telephone lines to handle demand.	Telephone Operators System Operators	Low	High	Avail.-High	IR-4, IR-5
A denial of service attack against the election official office jams fax machines and/or telephone lines.	Telephone Operators Hostile Organizations	Mod.	High	Avail.-High	IR-4, IR-5, CP-7, CP-8, SC-5
Personally identifiable material is intercepted en route.	Telephone Operators Hostile Organizations	High	Low	Confid.-Mod.	PE-4, SC-8, SC-9, SC-12, SC-13
Election officials are flooded with a large number of illegitimate faxed ballots.	Hostile Organizations	Mod.	High	Avail-Mod. Integrity-Mod.	IR-4, IR-5
An attacker tricks voters into calling the wrong phone number to vote.	Hostile Individual Hostile Organization	Low	High	Integrity-High	<i>Outside control of officials.</i>
Disgruntled election official fails to properly handle faxed ballots.	Election Official	Mod.	Low	Integrity-Mod.	PS-2, PS-3
Sensitive personal information and/or ballot selections are improperly read from faxed votes.	Election Officials Support Staff Hostile Individuals	Mod.	Mod.	Confid.-Mod	PE-2, PE-3, PE-5, PE-6, PS-2, PS-3
Sensitive personal information and/or ballot selections are improperly read from received ballots in storage.	Election Officials	Mod.	Mod.	Confid.-High	MP-1, MP-2, MP-4, PE-2, PE-3, PE-6, PS-2, PS-3
Electronic copies of faxed ballots are read of the memory of fax machines.	Hostile Individuals	High	Low	Confid.-Mod.	<i>Largely outside the control of officials.</i>

**Table 13: Threat Matrix for Fax Ballot Return**

Denial of service attacks may be possible against these systems. Malicious groups could flood election fax machines with large numbers of illegitimate ballots. Such an attack would have two major results. First, the illegitimate traffic could tie up communication lines, preventing legitimate voters from casting ballots. Second, it may be difficult for election officials to distinguish the legitimate ballots from the illegitimate ballots. Postal mail distribution and return of ballots could limit the number of forged ballots since valid inbound ballots would need to be on the proper paper stock; however, there would be no such protection with faxed ballots. Illegitimate votes would have to be identified using the voter identification and authentication information (e.g. a voter’s signature), possibly with the assistance of any ballot tracking information. A small number of illegitimate ballots may be able to pass through these checks.

### 6.3.4 Electronic Mail

In most instances, voted ballots returned via e-mail would reach election officials nearly instantaneously. Communications could, however, be disrupted by malicious parties. Denial of service attacks are a significant threat to e-mail-based voting systems. Attackers could flood election e-mail servers with large amounts of illegitimate traffic. This could not only prevent voters’ e-mails from reaching election officials, but could also make it difficult for officials to distinguish between valid and invalid ballots.

Eavesdropping is a potential threat whenever Internet communications is involved, and particularly with e-mailed communications, which are sent unencrypted. While eavesdropping is

not a significant threat for ballot distribution, as that information is generally publically available, voted ballots must remain confidential. Voted ballots show how an individual voted, and may sometimes contain sensitive personal information about the voter. E-mails are significantly easier to intercept and modify in transit than other forms of communication. E-mails travel through telecommunications lines, network equipment and e-mail servers before reaching the intended recipient. Anyone with access to the infrastructure could read or even modify e-mail messages. In particular, e-mail servers often store messages for a short period of time before passing them on to the next server, or the intended recipient. System operators for these servers could intercept or modify e-mailed ballots. It is unlikely that election officials would be able to identify ballots that had been modified in-transit.

Also, e-mailed ballots are at risk before and after they are sent to election officials. Voters' computers could be infected with malicious code capable of disrupting communications with an election official. Very sophisticated attacks may be able to modify digital ballots prior to e-mailing them to election officials. Malicious code would need to spread to a large number of personal computers before it would have a substantial effect on an election. The computer virus may be detected before election day, but there would be no way for election officials to identify affected ballots. Similar malicious code on election computer systems could have the same effect.

E-mail does not provide any guarantee that the intended recipient will receive the message. The e-mail system relies on the DNS system [11] to route e-mails to the proper servers. An attack on DNS servers could route e-mails to an attacking party. This would not only result in voter disenfranchisement, but also the loss of sensitive voter information. This kind of attack would require very sophisticated attackers focusing their efforts on major e-mail service providers. There are no known reports of a similar attack being successfully conducted on e-mail or DNS servers. However, it is important to note that a recent vulnerability was discovered in DNS servers that could have been used to construct a similar attack [13]. DNS servers were quickly patched before any significant attack took place.

Less sophisticated, but equally effective, attacks may attempt to trick voters into sending their ballots to an attacker. That is, an attacker would contact a large number of voters, claiming to be their local election official and attempting to convince them to reply with their cast ballot. While a relatively small number of voters may be fooled, it is relatively easy and cheap to contact a very large numbers of voters.



Threat	Threat-Sources	Effort	Detection	Impact	Possible Controls
Impersonation of registered voter (e.g., forged signature)	Hostile Individuals	Mod.	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5, IA-7
Voter coerced into voting a particular way	Hostile Individuals Hostile Organizations	Low	Mod	Confid.-Mod	<i>Outside control of officials.</i>
A denial of service attack against voter and/or election official e-mail servers overwhelms resources and prevents the transmission of voted ballots	Hostile Organizations	Mod.	High	Avail-High	IR-4, IR-5, CP-7, CP-8, SC-5
Election official offices have too few resources (e.g., bandwidth, servers) to handle legitimate traffic	Network Operators Election Officials	Low	High	Avail-High	IR-4, IR-5
Sensitive personal information or ballot selections are intercepted between the voter and election official on the Internet	Hostile Organizations Network Operators	High	Low	Confid.-Mod	PE-4, SC-9, SC-12, SC-13
Voted ballots are modified while being transmitted to the election official (e.g. on e-mail servers)	Hostile Organizations Network Operators	High	Low	Integrity-Mod	SC-8, SC-12, SC-13
Malicious code (e.g., a Trojan horse) on a voter's computer modifies or disrupts outgoing e-mails containing voted ballots	Hostile Individuals Hostile Organizations	High	Mod.	Integrity-Mod	<i>Outside control of officials.</i>
Voter ballot selections are accessed off election information systems by individuals with authorized access to these machines, resulting in loss of voter privacy	System Operators Election Officials	Mod.	Low	Confid.-High	PE-2, PE-3, PE-6, PS-2, PS-3, AU-2, AU-3, AU-4, AU-6, AU-7, AU-8, AU-9, AU-10, AC-2, AC-3, AC-5, AC-6
Voter ballot selections are accessed off election information systems by unauthorized personnel, resulting in loss of voter privacy	Hostile Individuals Election Officials	High	Low	Confid.-High	AC-2, AC-3, IA-2, PE-2, PE-3, PE-5, PE-6, PS-2, PS-3
Individuals with physical access to election information systems delete or modify ballots stored on these systems	Hostile Individual System Operators Election Official	High	Low	Integrity-High	AC-2, AC-3, IA-2, PE-2, PE-3, PE-5, PE-6, PS-2, PS-3
Unauthorized individuals remotely access election information systems and view, modify or delete ballots stored on these systems	Hostile Individuals Hostile Organizations	High	Mod	Confid.-High Integrity-High	AC-2, AC-3, IA-2, SC-7, SC-8, SC-13, SI-4
Malicious code (e.g. a Trojan horse) on the voter's e-mail server modifies or deletes e-mails containing voted ballots	Hostile Individuals Hostile Organizations	High	Low	Integrity-Mod.	<i>Outside control of officials.</i>
Malicious code (e.g. spyware) on the voter's e-mail server transmits voter ballot selections to a third party	Hostile Individuals Hostile Organizations	High	Low	Confid.-Mod.	SC-9, SC-13 <i>Largely outside control of officials.</i>
Malicious code (e.g., a Trojan horse) on the election official's e-mail server modifies or deletes e-mails containing voted ballots	Hostile Individuals Hostile Organizations	High	Mod.	Integrity-High	IA-2, AC-3, CM-3, CM-5, MA-2, MA-3, MA-5, SI-3, SI-4, SI-7, PE-2, PE-3, PS-2, PS-3, SC-7, SC-8, SC-13
Malicious code (e.g., spyware) on the election official's e-mail server transmits voter ballot selections to a third party	Hostile Individuals Hostile Organizations	High	Mod.	Confid.-High	IA-2, AC-3, CM-3, CM-5, MA-2, MA-3, MA-5, SI-3, SI-4, SI-7, PE-2, PE-3, PS-2, PS-3, SC-7, SC-9, SC-13
Disgruntled election officials fail to properly record the e-mailed vote	Election Official	Mod.	Low	Integrity-Mod.	PS-2, PS-3
An individual reads, modifies or destroys an e-mailed ballot in storage, after it has been printed, but before being tallied	Election Official	Mod.	Mod.	Confid.-High Integrity-High	PS-2, PS-3, PE-2, PE-3, MP-1, MP-2, MP-4
Voters are tricked into sending voted ballots to an incorrect e-mail address, resulting in the disenfranchisement and the loss of personal information	Hostile Individual Hostile Organization	Low	High	Confid.-High Avail.-Mod.	<i>Outside control of officials.</i>
An attack on the DNS system causes e-mails containing voted ballots to be sent to attackers.	Hostile Individual Hostile Organization	Mod.	High	Confid.-High Avail.-Mod.	<i>Largely outside control of officials.</i>

**Table 14: Threat Matrix for E-mail Ballot Return**

### 6.3.5 Web-Based

Web-based Internet voting is a form of electronic voting. The election web server would need to be trusted to accurately record voters' selections. Defects in the voting system software, or malicious code installed on the voting system by hostile individuals, could cause votes to be recorded improperly, or could modify votes at a later time. Skilled hackers may find vulnerability in the voting system software that would grant them access to voter and ballot information. This could also lead to a loss of voter secrecy, or a loss of election integrity. Sophisticated attacks would leave little or no evidence.

Election officials, or other individuals with physical access to voting system equipment, may be able to gain access to election information, including cast ballots. Sophisticated attackers may also be able to delete any audit records that would leave evidence of their attack.

Denial of service attacks are significant threats to Internet-based voting systems. A successful denial of service attack would overwhelm the election web server with traffic, preventing legitimate voters from casting a ballot. It is very difficult to protect against denial of service attacks from an attacker with a large amount of resources. A successful denial of service attack generally requires access to a large number of computers with high-speed Internet connections. While an attacking organization may purchase these systems, it typically would use a Botnet. A Botnet is a collection of personal computers that have been infected with a virus that gives an attacker control of the computer. Control of Botnet-infected computers is sold on the black market, given nearly anyone with financial resources the technical resources to perform a denial of service attack.

Many of the potential threats to a web-based Internet voting system involve attacks on equipment that are not under election officials' control. Attacks on the DNS system could lead voters to fraudulent web sites. These voters may unknowingly provide their voter credentials to a malicious party, who in turn could impersonate the voter on the legitimate election server. Malicious code installed on voters' personal computers could disrupt communications with an election web server, or even modify voters' ballot choices without their knowledge. A computer virus would have to spread to a large number of computers before it could have a substantial effect on an election. Antivirus vendors may be able to identify and offer protections against such viruses, but not until after some voters' computers have been compromised. Furthermore, election officials would have no guarantee that their constituents would use updated anti-virus software. Election officials would have little recourse but to assume that all received votes are valid, as there would be no way to identify ballots from compromised machines.

Less sophisticated attackers may be able to trick voters into navigating to a fraudulent web site that would mimic the actual election site. This type of attack, known as phishing, involves sending a large number of messages to potential voters claiming to be from election officials. The message could instruct voters to log into the fraudulent web site to cast a ballot. While most voters would discard such messages, a small percentage of voters could fall victim to this attack, which is common in the banking industry.

Threat	Threat-Sources	Effort	Detection	Impact	Possible Controls
Impersonation of registered voter.	Hostile Individuals	Mod.	Mod.	Integrity-Mod.	IA-1, IA-2, IA-4, IA-5, IA-7
Voter coerced into voting a particular way.	Hostile Individuals Hostile Organizations	Low	Mod	Confid.-Mod	<i>Outside control of officials.</i>
A denial of service attack against the election web servers overwhelms resources and prevents the transmission of voted ballots.	Hostile Organizations	Low	High	Avail-High	IR-4, IR-5, CP-7, CP-8, SC-5
Election official offices have too few resources (e.g. bandwidth, servers) to handle legitimate traffic.	Network Operators Election Officials	Low	High	Avail-High	IR-4, IR-5
Personal information is intercepted between the voter and election official on the Internet.	Hostile Organizations Network Operators	High	Low	Confid.-High	PE-4, SC-6, SC-7, SC-12, SC-13
Malicious code (e.g., a Trojan horse) on a voter's computer modifies communication with the election web server, modifying voted ballots before passing them to the server.	Hostile Individual Hostile Organization	High	Mod.	Integrity-Mod.	<i>Outside control of officials.</i>
Malicious code (e.g., a Trojan horse) on a voter's computer disrupts communication with the election web server, preventing ballot return.	Hostile Individual Hostile Organization	High	Mod.	Avail.-Mod.	<i>Outside control of officials.</i>
Voter ballot selections are accessed off election information systems by individuals with authorized access to these machines, resulting in loss of voter privacy.	System Operators Election Officials	Mod.	Low	Confid.-High	PE-2, PE-3, PE-6, PS-2, PS-3, AU-2, AU-3, AU-4, AU-6, AU-7, AU-8, AU-9, AU-10, AC-2, AC-3, AC-5, AC-6
Voter ballot selections are accessed off election information systems by unauthorized personnel, resulting in loss of voter privacy.	Hostile Individuals Election Officials	High	Low	Confid.-High	AC-2, AC-3, IA-2, PE-2, PE-3, PE-5, PE-6, PS-2, PS-3
Individuals with physical access to election information systems delete or modify ballots stored on these systems	Hostile Individual System Operators Election Official	High	Low	Integrity-High	AC-2, AC-3, IA-2, PE-2, PE-3, PE-5, PE-6, PS-2, PS-3
Unauthorized individuals remotely access election information systems and view, modify or delete ballots stored on these systems	Hostile Individuals Hostile Organizations	High	Mod	Confid.-High Integrity-High	AC-2, AC-3, IA-2, SC-7, SI-4
Malicious code (e.g. a Trojan horse) on the election web server deletes or modifies voted ballots.	Hostile Individual Hostile Organization	High	Mod.	Integrity-High	IA-2, AC-3, CM-5, MA-2, MA-3, MA-5, SI-3, SI-4, SI-7, PE-2, PE-3, PS-2, PS-3
Malicious code (e.g., spyware) on the election web server transmits voter ballot selections to a third party.	Hostile Individual Hostile Organization	High	Mod.	Confid.-High	IA-2, AC-3, CM-5, MA-2, MA-3, MA-5, SI-3, SI-4, SI-7, PE-2, PE-3, PS-2, PS-3
Malicious code (e.g., spyware) on a voter's computer transmits voter ballot selections to a third party.	Hostile Individual Hostile Organization	High	Mod.	Confid.-Mod.	<i>Outside control of officials.</i>
Defects in the voting system server software cause votes to be recorded incorrectly	System Manufacturers	Mod.	Low	Integrity-High	SI-2, CM-2, CM-3, CM-5
Voters are tricked into returning voted ballots via an incorrect web site (e.g. through Phishing), resulting in the disenfranchisement and the loss of personal information.	Hostile Organizations	Low	High	Integrity-High Confid.-High	<i>Outside control of officials.</i>
An attack on the DNS system forwards voters to an incorrect website, resulting in the disenfranchisement and the loss of personal information.	Hostile Organizations	High	High	Integrity-High	<i>Largely outside control of officials.</i>

Table 15: Threat Matrix for Web-Based Ballot Return

## 7 Security Controls

The threat analysis conducted and documented in Section 6 includes references to security controls. These controls provide procedural and technical countermeasures to protect the confidentiality, integrity and availability of systems from threats. Whenever possible, specific controls are referenced for each threat identified in the analysis. These controls fully or partially mitigate the associated threat. In some cases the controls are preventative. That is, the controls prevent a security violation from taking place. In other cases the controls are reactive, in that they help recover from an attack or other security violation without further loss of confidentiality, integrity or availability. Preventative controls are preferable, but not always possible or realistic.

This section summarizes the security controls identified to mitigate threats to each transmission option. These controls point to specific controls listed in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* [3]. NIST SP 800-53 is a catalog of high-level security controls, written primarily for federal computer systems. This report references the controls documented in NIST SP 800-53 by the Control Number. As the controls are high-level, and not geared for election systems, this report includes discussion on how these controls could be implemented in UOCAVA election systems.

The particular security controls referenced in this report mitigate specific threats identified to each transmission option. Furthermore, threats are identified for the high-level characterizations of election systems outlined in Section 4. Most jurisdictions will use a variation of one or more of the systems identified in this paper. As such, specific voting systems may be vulnerable to different threats, requiring a different set of security controls. This report does not suggest that the following controls adequately mitigate the threats faced by each system. Individual jurisdictions should use threats and security controls in this report, along with specific information about their own systems and accompanying procedures, to ensure adequate security controls are in place. Furthermore, election systems should be designed with good security engineering principles, which may dictate additional security controls than those specified here. For instance, auditing functionality, an important component of any secure computer system, may not effectively mitigate any specific threat on its own, but it would provide useful information when responding to malicious attacks or simple malfunctions.

## 7.1 Postal Mail

Ctrl. Name	Stages			Control Text	Notes
	RBR <sup>1</sup>	BD <sup>2</sup>	BR <sup>3</sup>		
AC-2		X		ACCOUNT MANAGEMENT	Databases and IT systems used to manage registration information should be protected with access control mechanisms.
AC-3		X		ACCESS ENFORCEMENT	
AC-5		X		SEPARATION OF DUTIES	
AC-6		X		LEAST PRIVILEGE	
IA-1	X		X	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	Officials should develop procedures and implement technical mechanisms to identify voters, election officials and system administrators. Procedures may be used to authenticate voters, while IT systems should include IA and access control mechanisms.
IA-2	X		X	USER IDENTIFICATION AND AUTHENTICATION	
IA-4	X		X	IDENTIFIER MANAGEMENT	
IA-5	X		X	AUTHENTICATOR MANAGEMENT	
IR-4		X	X	INCIDENT HANDLING	Officials should monitor for disruptions in their IT systems and in external essential systems, such as postal mail delivery.
IR-5		X	X	INCIDENT MONITORING	
MP-1	X	X	X	MEDIA PROTECTION POLICY AND PROCEDURES	Officials should protect registration forms, blank paper ballots and voted ballots with procedures. Care should be taken when transporting these materials, both internally and via the postal service.
MP-2	X	X	X	MEDIA ACCESS	
MP-4	X	X	X	MEDIA STORAGE	
MP-5	X	X	X	MEDIA TRANSPORT	
PE-2	X	X	X	ACCESS CONTROL FOR TRANSMISSION MEDIUM	Officials should control physical access to vital systems and sensitive information.
PE-3	X	X	X	MONITORING PHYSICAL ACCESS	
PS-2	X	X	X	POSITION CATEGORIZATION	Screen election employees who will be handling registration forms and ballots.
PS-3	X	X	X	PERSONNEL SCREENING	

### *Access Control (AC):*

IT systems containing important election information, such as an electronic voter registration database should be protected by access control mechanisms. Access to these systems should be limited to employees who need this information to perform election-related duties. Furthermore, individuals who need access to some voter information should not necessarily be granted access to all information. For example, an individual charged with mailing blank ballots needs access to voter names, addresses and residency information, but may not need access to sensitive voter information used for authentication purposes. Officials should regularly review their access control policies and make appropriate changes as the individuals' responsibilities change.

### *Identity and Authentication (IA):*

Officials should develop technical and procedural mechanisms to identify all users of the election system, including voters, election officials and system administrators. Voter authentication in postal mail systems is largely done via procedural mechanisms. Individual jurisdictions must determine appropriate voter authentication mechanisms. Initial voter

<sup>1</sup> Registration and Ballot Return

<sup>2</sup> Ballot Delivery

<sup>3</sup> Ballot Return

authentication occurs in the registration phase, where some type of authenticator (typically a voter signature) is exchanged. This authenticator must be securely stored by election officials so that it is available to authenticate future correspondence from a voter. While some authenticators, such as PINs, are easy to verify, training is necessary to verify authenticators like voter signatures.

Authentication on election IT systems should be automated and tied to the systems' access control and auditing mechanisms. Systems should identify and authenticate each individual with access to a system, usually through a user name and password. Jurisdictions should develop appropriate policies regarding the use of passwords for authentication, including setting password complexity requirements and expiration times, or the use of biometrics.

***Incident Response (IR):***

Election officials should monitor vital necessary election components to ensure they are functioning properly. Postal mail systems may use a combination of computer and manual systems and procedures. Officials should monitor audit records of electronic voter registration databases and automated ballot tracking systems. Officials should also continuously monitor access to physical storage locations of registration forms and ballots. Also, officials should monitor the status of the postal mail system, watching for current mail disruptions and events which could cause disruptions in the future. While it may be difficult to recover from events in a current election, detected incidents may suggest important technical and procedural controls for future elections.

***Media Protection (MP):***

Examples of election media in postal mail election systems are registration forms, blank ballots and voted ballots, all of which are on paper. Access to these forms and ballots should be tightly controlled. This media should be stored in a secure location. Only election officials involved with the absentee voting process should have access to this physical location, and any accesses should be logged procedurally or, preferably, automatically.

Officials have limited control of registration forms and ballots in the mail. However, officials should track items, particularly ballots, through the mail whenever possible. A number of deployed absentee ballot management systems exist which provide ballot tracking capabilities. This functionality is not only useful for tracking ballots through the mail, but also throughout the entire voting process, from ballot casting to counting. Such tracking systems can mitigate a large number of internal and external threats to postal mail election systems. However, they also present a privacy risk. Ballot tracking systems should implement procedural and technical controls which can be used to maintain voter privacy.

***Physical Security (PE):***

As discussed, it is important to limit physical access to election systems and voter information. Physical access to storage locations of registration forms and ballots, inbound and outbound mail boxes and vital election IT systems should be limited to only those who need access to perform their election-related duties. Access could be limited using locks and/or keycards. Whenever possible, access to these locations should be logged.

***Personnel Security (PS):***

A malicious election official or system administrator could attack a postal mail system in a variety of ways. Jurisdictions should categorize the various roles in their election process according to the level of access to voter information and ballots. Whenever possible, the confidentiality, integrity or availability of the election system should not depend on a single individual. However, that may be infeasible. Some individuals, such as the person charged with addressing and mailing blank ballots, could inflict harm on the system, and it may not be feasible to do all tasks in pairs. In such instances, jurisdictions should do whatever is necessary to gain confidence that that individual will perform his or her duties appropriately. This may include some kind of background screening process.

## 7.2 Telephone Transmission

Ctrl. Number	Stages <sup>4</sup>		Control Text	Notes:	
	RB	BR			
AC-2		X	ACCOUNT MANAGEMENT	IT systems used to manage registration information and interact with voters using telephone lines should be protected with access control mechanisms.	
AC-3		X	ACCESS ENFORCEMENT		
AC-5		X	SEPARATION OF DUTIES		
AC-6		X	LEAST PRIVILEGE		
AU-2		X	AUDITABLE EVENTS	Election systems should include auditing functionality to determine the actions of users. This should be done via automated means on IT systems, such as the electronic registration database and telephone voting server, or via procedural methods to record manual actions by election officials.	
AU-3		X	CONTENT OF AUDIT RECORDS		
AU-4		X	AUDIT STORAGE CAPACITY		
AU-6		X	AUDIT MONITORING, ANALYSIS, AND REPORTING		
AU-7		X	AUDIT REDUCTION AND REPORT GENERATION		
AU-8		X	TIME STAMPS		
AU-9		X	PROTECTION OF AUDIT INFORMATION		
AU-10		X	NON-REPUDIATION		
CM-2		X	BASELINE CONFIGURATION		System administrators should closely monitor the configuration of vital IT systems to ensure they have not been manipulated.
CM-3		X	CONFIGURATION CHANGE CONTROL		
CM-5		X	ACCESS RESTRICTIONS FOR CHANGE		
CP-7	X	X	ALTERNATE PROCESSING SITE	Officials should prepare a backup telecommunications system in case of an unscheduled outage or attack.	
CP-8	X	X	TELECOMMUNICATIONS SERVICES		
IA-1	X	X	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	Officials should develop procedures and implement technical mechanisms to identify voters, election officials and system administrators. Procedures may be used to authenticate voters, while IT systems should include IA and access control mechanisms.	
IA-2	X	X	USER IDENTIFICATION AND AUTHENTICATION		
IA-4	X	X	IDENTIFIER MANAGEMENT		
IA-5	X	X	AUTHENTICATOR MANAGEMENT		
IA-7	X	X	CRYPTOGRAPHIC MODULE AUTHENTICATION		
IR-4	X	X	INCIDENT HANDLING	Officials should monitor their IT systems and communications services for disruptions and possible attacks.	
IR-5	X	X	INCIDENT MONITORING		
MA-2		X	CONTROLLED MAINTENANCE	System administrators should closely monitor the maintenance of vital IT systems to ensure the proper hardware and software updates are performed on such systems.	
MA-3		X	MAINTENANCE TOOLS		
MA-5		X	MAINTENANCE PERSONNEL		
PE-2	X	X	PHYSICAL ACCESS AUTHORIZATIONS	Officials should control physical access to vital systems and sensitive information. This includes physical access to IT systems and communications equipment.	
PE-3	X	X	PHYSICAL ACCESS CONTROL		
PE-4	X	X	ACCESS CONTROL FOR TRANSMISSION MEDIUM		
PE-5	X	X	ACCESS CONTROL FOR DISPLAY MEDIUM		
PE-6	X	X	MONITORING PHYSICAL ACCESS		

<sup>4</sup> Telephones are not used to create a ballot delivery system. Telephone voting systems provide voters with ballot questions, along with a mechanism to submit votes. As such, telephone voting systems are considered a type of ballot return system.



Ctrl. Number	Stages <sup>4</sup>		Control Text	Notes:
	RB	BR		
PS-2	X	X	POSITION CATEGORIZATION	Screen election employees who will be administering IT systems or receiving/transcribing voter information.
PS-3	X	X	PERSONNEL SCREENING	
SC-5	X	X	DENIAL OF SERVICE PROTECTION	Officials must develop protections against denial of service attacks and mitigate the effect with backup procedures.  Whenever possible, information sent over telephone lines should have integrity and confidentiality protection. This may be possible with kiosks with secure telephones.
SC-8	X	X	TRANSMISSION INTEGRITY	
SC-9	X	X	TRANSMISSION CONFIDENTIALITY	
SC-12	X	X	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
SC-13	X	X	USE OF CRYPTOGRAPHY	
SI-2		X	FLAW REMEDIATION	System administrators should watch for defects and malicious code in IT systems that could prevent those systems from functioning properly.
SI-3		X	MALICIOUS CODE PROTECTION	
SI-4		X	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES	
SI-7		X	SOFTWARE AND INFORMATION INTEGRITY	

***Access Control (AC):***

Most telephone-based voting systems contain at least two vital computer systems: an electronic voter registration database and the telephone voting server, which connects to the telephone network and interacts with voters. Both of these systems need to be protected by access control mechanisms. Access to these systems should be limited to employees who need the information on the system to perform election-related duties. If election officials are communicating directly with voters registering or requesting ballots, several officials may need access to the database. Fewer individuals should need access to the information on the telephone voting server, as it automates the process of interacting with voters. Officials should regularly review their access control policies and make appropriate changes as individuals' responsibilities change.

***Audit and Accountability (AU):***

Election computer systems should keep audit records of important events on the system, such as authentication attempts, maintenance and other administrative activities, and voter sessions. The audit records should provide enough information to determine who performed a given action, a description of the action, and the time it took place.

Maintaining the integrity of this information is important, and systems should implement controls which protect audit information from unauthorized access, modification or deletion. The security control AU-9(1) listed in NIST SP-800-53 suggests that audit records be produced on hardware-enforced, write-once media. This control, or variations of it, is highly recommended for important election records, such as votes. Systems could print certain kinds of election records on paper, and store them in a secure box. Alternatively, systems could implement cryptographic protections, such as signing records using validated hardware cryptographic modules validated under FIPS-140, Security Requirements for Cryptographic Modules, procedures.

***Configuration Management (CM):***

The integrity of votes in a telephone voting system is dependent on the software in the telephone voting server. System administrators should have a baseline configuration for the election system, and access control mechanisms should prevent anyone other than authorized system administrators from making any changes to this configuration. All changes should be recorded in the audit log for the system.

***Contingency Planning (CP):***

Backup plans and systems should be developed and implemented in the event that telephone service drops due to increased demand, outages, or attacks.

***Identity and Authentication (IA):***

Officials should develop technical and procedural mechanisms to identify all users of the election system, including voters, election officials and system administrators. Voter authentication in registration systems is largely done via procedural mechanisms. Individual jurisdictions must determine appropriate voter authentication mechanisms. Initial voter authentication occurs in the registration phase, where some type of authenticator is exchanged. In the case of telephone voting systems, the voter authenticator is likely a PIN. This authenticator must be securely stored by election officials so that it is available to authenticate future correspondence from a voter.

Authentication on election IT systems should be automated and tied to the systems' access control and auditing mechanisms. Systems should identify and authenticate each individual with access to a system, usually through a user name and password. Jurisdictions should develop appropriate policies regarding the use of passwords for authentication, including setting password complexity requirements and expiration times.

***Incident Response (IR):***

Election officials should monitor vital necessary election systems and communications services to ensure they are functioning properly. Officials should monitor audit records of electronic voter registration databases and telephone voting system servers. Officials should also continuously monitor physical access to these systems. To protect against unscheduled service outages and denial of service attacks, administrators should closely monitor the status of the telephone lines used to register voters and submit votes, and implement contingency plans when necessary.

***Maintenance (MA):***

Telephone voting systems rely on software to ensure that votes are recorded properly. Due to potential software defects, it is important for jurisdictions to develop and follow appropriate controls to see that software updates are installed when needed. Because of the threat of malicious code, it is important that these controls ensure that only proper software updates are installed, and that these updates are installed by authorized system administrators.

***Physical Security (PE):***

It is important to limit physical access to election systems and voter information. Individuals with physical access to election computer systems may be able to access sensitive records, modify records or software, or cause equipment to fail. Access to areas containing vital election

systems should be limited to only those who need access to perform their election-related duties. Access could be limited using locks and/or keycards. Whenever possible, access to these locations should be logged.

***Personnel Security (PS):***

A malicious election official or system administrator may have access to vital election system equipment or information. Jurisdictions should categorize the various roles in their election process according to the level of access to voter information and ballots. Whenever possible, the confidentiality, integrity or availability of the election system should not depend on a single individual. However, that may not be feasible. One jurisdiction may not have multiple employees capable of acting as system administrators for the electronic registration database or the telephone voting server. Jurisdictions should take appropriate actions to gain confidence that that individual will perform his or her duties appropriately. This may include some kind of background screening process.

***System and Communications Protection (SC):***

Sensitive or critical information transmitted over a public communications network typically should have cryptographic protections in order to protect the confidentiality and/or integrity of transmitted data. However, such protections could not be implemented without preventing voters with standard telephones from using the telephone voting system. An alternative is for jurisdictions to set up kiosks with secure telephones. Voters would not be able to vote from their home telephones; instead they would have to go to a kiosk and vote from one of the terminals. Individual jurisdictions must weigh the risks of eavesdropping and modifications in transit against the convenience of telephone voting from home.

***System and Information Integrity (SI):***

As previously noted, telephone voting systems rely on the correctness of software running on the telephone voting server. System administrators should test and monitor their systems to look for defects in the system that could prevent votes from being recorded properly, disrupt the elections, or release sensitive information to an attacker. Furthermore, election computer systems should be protected from malicious code using antivirus software. Systems connected to a network should be protected with a firewall and an intrusion detection system (IDS). In most cases the firewall and IDS will be separate devices on the jurisdiction's computer network.

### 7.3 Fax Transmission

Ctrl. Number	Stages			Control Text	Notes
	RB	BD	BR		
AC-2		X		ACCOUNT MANAGEMENT	Databases and IT systems used to manage registration information should be protected with access control mechanisms.
AC-3		X		ACCESS ENFORCEMENT	
AC-5		X		SEPARATION OF DUTIES	
AC-6		X		LEAST PRIVILEGE	
CP-7	X		X	ALTERNATE PROCESSING SITE	Officials should prepare a backup telecommunications system in case of an unscheduled outage or attack.
CP-8	X		X	TELECOMMUNICATIONS SERVICES	
IA-1	X		X	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	Officials should develop procedures and implement technical mechanisms to identify voters, election officials and system administrators. Procedures may be used to authenticate voters, while IT systems should include IA and access control mechanisms.
IA-2	X		X	USER IDENTIFICATION AND AUTHENTICATION	
IA-4	X		X	IDENTIFIER MANAGEMENT	
IA-5	X		X	AUTHENTICATOR MANAGEMENT	
IA-7	X		X	CRYPTOGRAPHIC MODULE AUTHENTICATION	
IR-4	X	X	X	INCIDENT HANDLING	Officials should monitor their IT systems and communications services for disruptions and possible attacks.
IR-5	X	X	X	INCIDENT MONITORING	
MP-1	X	X	X	MEDIA PROTECTION POLICY AND PROCEDURES	Officials should protect registration forms, blank paper ballots and voted ballots with procedures.
MP-2	X	X	X	MEDIA ACCESS	
MP-4	X	X	X	MEDIA STORAGE	
PE-2	X	X	X	PHYSICAL ACCESS AUTHORIZATIONS	Officials should control physical access to vital systems and sensitive information. This includes physical access to IT systems and communications equipment.
PE-3	X	X	X	PHYSICAL ACCESS CONTROL	
PE-4			X	ACCESS CONTROL FOR TRANSMISSION MEDIUM	
PE-6	X		X	MONITORING PHYSICAL ACCESS	
PS-2	X	X	X	POSITION CATEGORIZATION	Screen election employees who will be handling registration forms and ballots.
PS-3	X	X	X	PERSONNEL SCREENING	
SC-5	X	X	X	DENIAL OF SERVICE PROTECTION	Officials must develop protections against denial of service attacks or mitigate the effect with backup procedures.
SC-8	X	X	X	TRANSMISSION INTEGRITY	
SC-9	X	X	X	TRANSMISSION CONFIDENTIALITY	Whenever possible, information sent over telephone lines should have integrity and confidentiality protection. This may be possible with kiosks holding secure fax machines.
SC-12	X	X	X	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
SC-13	X	X	X	USE OF CRYPTOGRAPHY	
SC-14		X		PUBLIC ACCESS PROTECTIONS	

#### *Access Control (AC):*

IT systems containing important election information, such as an electronic voter registration database should be protected by access control mechanisms. Access to these systems should be limited to employees who need this information to perform election-related duties. Furthermore, individuals who need access to some voter information should not necessarily be granted access to all information. Officials should regularly review their access control policies and make appropriate changes as individuals' responsibilities change.

***Contingency Planning (CP):***

Backup plans and systems should be developed and implemented in the event that telephone service drops due to increased demand, outages, or attacks.

***Identity and Authentication (IA):***

Officials should develop technical and procedural mechanisms to identify all users of the election system, including voters, election officials and system administrators. Voter authentication in fax systems is largely done via procedural mechanisms. Individual jurisdictions must determine appropriate voter authentication mechanisms. Initial voter authentication occurs in the registration phase, where some type of authenticator (typically a voter signature) is exchanged. This authenticator must be securely stored by election officials so that it is available to authenticate future correspondence from a voter. While some authenticators, such as PINs, are easy to verify, training is necessary to verify authenticators like voter signatures.

Authentication on election IT systems should be automated and tied to the systems' access control and auditing mechanisms. Systems should identify and authenticate each individual with access to a system, usually through a user name and password. Jurisdictions should develop appropriate policies regarding the use of passwords for authentication, including setting password complexity requirements and expiration times.

***Incident Response (IR):***

Election officials should monitor vital necessary election systems, such as the voter registration database, and communications services to ensure they are functioning properly. Officials should also continuously monitor physical access to these systems. To protect against unscheduled service outages and denial of service attacks, administrators should closely monitor the status of the telephone lines used to receive faxed requests and ballots, and implement contingency plans when necessary.

***Media Protection (MP):***

Examples of election media in election systems are registration forms, blank ballots and voted ballots, all of which are on paper prior to and after being faxed. Access to these forms and ballots should be tightly controlled. This media should be stored in a secure location. Only election officials involved with the absentee voting process should have access to this physical location, and any accesses should be logged procedurally or, preferably, automatically. Specifically, registration forms and voted ballots received via fax are at-risk to being read or modified by anyone in the vicinity of the fax machine. Fax machines that will receive election materials should be kept in a locked room.

Election materials in fax-based systems will experience two or more conversions from being a physical entity to an electronic signal, or vice versa. While paper-based systems can use unique ballot stock to help identify clearly forged ballots, this is not possible in a fax-based system. Attackers could make multiple copies of ballots, using them to flood election official offices or perform other attacks. Ballot tracking systems, such as those described Section 6.1, could help mitigate this threat, while also helping ensure paper copies of faxed ballots are not lost in the

counting process. The systems used with postal ballots should be able to be used with minor modifications.

***Physical Security (PE):***

It is important to limit physical access to election systems and voter information. As previously noted, individuals with physical access to fax machines may be able to read sensitive voter information, violate voter privacy or modify received votes. Access to areas containing vital election systems, including fax machines and voter registration databases, should be limited only to those who need access to perform their election-related duties. Access could be limited using locks and/or keycards. Whenever possible, access to these locations should be logged.

***Personnel Security (PS):***

As previously discussed, a malicious election official or system administrator could attack a fax-based election system in a variety of ways. Jurisdictions should categorize the various roles in their election process according to the level of access to voter information and ballots. Whenever possible, the confidentiality, integrity or availability of the election system should not depend on a single individual. However, that may not be feasible. Some individuals, such as the person charged with faxing blank ballots, could inflict harm on the system, and it may not be feasible to do all tasks in pairs. In such instances, jurisdictions should do whatever is necessary to gain confidence that that individual will perform his or her duties appropriately. This may include some kind of background screening process.

***System and Communications Protection (SC):***

Sensitive or critical information transmitted over a public communications network may have cryptographic protections in order to protect the confidentiality and/or integrity of transmitted data. However, such protections could not be implemented without preventing voters with a standard fax machine from using the system. An alternative is for jurisdictions to set up kiosks with secure fax machines. Voters would not be able to vote from their home fax machines; instead they would have to go to a kiosk and vote from one of the terminals. Individual jurisdictions must weigh the risks of eavesdropping and modifications in transit against the convenience of voting using a fax machine at home.

### 7.4 E-Mail Transmission

Ctrl. No.	Stages			Control Name	Notes	
	RB	BD	BR			
AC-2	X	X	X	ACCOUNT MANAGEMENT	IT systems used to manage registration information, election workstations, and local e-mail servers should be protected with access control mechanisms.	
AC-3	X	X	X	ACCESS ENFORCEMENT		
AC-5	X	X	X	SEPARATION OF DUTIES		
AC-6	X	X	X	LEAST PRIVILEGE		
AC-12	X			SESSION TERMINATION		
AU-2			X	AUDITABLE EVENTS	Election systems should include auditing functionality to determine. E-mail servers, election workstations, and registration databases should have system event logging functionality. Procedural methods should be used to record manual actions by election officials.	
AU-3			X	CONTENT OF AUDIT RECORDS		
AU-4			X	AUDIT STORAGE CAPACITY		
AU-6			X	AUDIT MONITORING, ANALYSIS, AND REPORTING		
AU-7			X	AUDIT REDUCTION AND REPORT GENERATION		
AU-8			X	TIME STAMPS		
AU-9			X	PROTECTION OF AUDIT INFORMATION		
AU-10			X	NON-REPUDIATION		
CM-2			X	BASELINE CONFIGURATION		System administrators should closely monitor the maintenance of vital IT systems to ensure the proper hardware and software updates are performed on such systems.
CM-3			X	CONFIGURATION CHANGE CONTROL		
CM-5			X	ACCESS RESTRICTIONS FOR CHANGE		
CP-7	X	X	X	ALTERNATE PROCESSING SITE	Officials should prepare a backup telecommunications system in case of an unscheduled outage or attack.	
CP-8	X	X	X	TELECOMMUNICATIONS SERVICES		
IA-1	X		X	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	Officials should develop procedures and implement technical mechanisms to identify voters, election officials and system administrators. Procedures may be used to authenticate voters, while IT systems should include IA and access control mechanisms.	
IA-2	X		X	USER IDENTIFICATION AND AUTHENTICATION		
IA-4	X		X	IDENTIFIER MANAGEMENT		
IA-5	X		X	AUTHENTICATOR MANAGEMENT		
IA-7	X		X	CRYPTOGRAPHIC MODULE AUTHENTICATION		
IR-4	X	X	X	INCIDENT HANDLING	Officials should monitor their IT systems and communications services for disruptions and possible attacks.	
IR-5	X	X	X	INCIDENT MONITORING		
MA-2			X	CONTROLLED MAINTENANCE	System administrators should closely monitor the maintenance of vital IT systems to ensure the proper hardware and software updates are performed on such systems.	
MA-3			X	MAINTENANCE TOOLS		
MA-5			X	MAINTENANCE PERSONNEL		
MP-1			X	MEDIA PROTECTION POLICY AND PROCEDURES	Officials should protect printed returned ballots with procedures.	
MP-2			X	MEDIA ACCESS		
MP-4			X	MEDIA STORAGE		
PE-2	X	X	X	PHYSICAL ACCESS AUTHORIZATIONS	Officials should control physical access to vital systems and sensitive information. This includes physical access to IT systems and communications equipment.	
PE-3	X	X	X	PHYSICAL ACCESS CONTROL		
PE-4	X		X	ACCESS CONTROL FOR TRANSMISSION MEDIUM		
PE-6			X	MONITORING PHYSICAL ACCESS		

Ctrl. No.	Stages			Control Name	Notes
	RB	BD	BR		
PS-2	X	X	X	POSITION CATEGORIZATION	Screen election employees who will be administering IT systems.
PS-3	X	X	X	PERSONNEL SCREENING	
SC-5	X		X	DENIAL OF SERVICE PROTECTION	Officials must develop protections against denial of service attacks or mitigate the effect with backup procedures. Information sent over e-mail should have integrity protection and, if possible, confidentiality protection.
SC-7	X	X	X	BOUNDARY PROTECTION	
SC-8		X	X	TRANSMISSION INTEGRITY	
SC-9	X		X	TRANSMISSION CONFIDENTIALITY	
SC-12	X		X	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
SC-13	X	X	X	USE OF CRYPTOGRAPHY	
SC-14	X	X		PUBLIC ACCESS PROTECTIONS	
SC-20	X	X	X	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	
SC-21	X	X	X	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	
SI-2	X		X	FLAW REMEDIATION	
SI-3	X		X	MALICIOUS CODE PROTECTION	
SI-4	X		X	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES	
SI-5		X	X	SECURITY ALERTS AND ADVISORIES	
SI-7	X		X	SOFTWARE AND INFORMATION INTEGRITY	

***Access Control (AC):***

E-mail-based voting systems contain several different computer systems vital to the election process. These include computer workstations used by election officials, voter registration databases, and local e-mail servers administered by the jurisdiction. All of these systems should be protected by access control mechanisms. Access to these systems should be limited to employees who need this information to perform election-related duties. Officials should regularly review their access control policies and make appropriate changes as individuals' responsibilities change.

***Audit and Accountability (AU):***

Election computer systems should keep audit records of important events on the system, such as authentication attempts, maintenance and other administrative activities, and voter sessions. The audit records should provide enough information to determine who performed a given action, a description of the action, and the time it took place.

Maintaining the integrity of this information is important, and systems should implement controls which protect audit information from unauthorized access, modification or deletion. The security control AU-9(1) listed in NIST SP-800-53 suggests that audit records be produced on hardware-enforced, write-once media. This control, or variations of it, is highly recommended for important election records, such as votes. Election officials should consider printing received ballots immediately, and storing them in a secure location. It should be noted,



however, that this would merely duplicate the results of many attacks, rather than prevent them. For instance, if voted ballots are modified before reaching the election official, printing the modified ballots would not prevent or detect the attack.

***Configuration Management (CM):***

The integrity of votes and the reliability of the system are dependent on the correctness of software in key computer systems supporting the election process. Computer workstations, voter registration databases and e-mail servers are all vital election computer systems. System administrators should have baseline configurations for these systems, and access control mechanisms should prevent anyone other than authorized system administrators from making any changes to these configurations. All changes should be recorded in the audit log for the system.

***Contingency Planning (CP):***

Backup plans and systems should be developed and implemented in the event that Internet service drops due to increased demand, outages, or attacks.

***Identity and Authentication (IA):***

Officials should develop technical and procedural mechanisms to identify all users of the election system, including voters, election officials and system administrators. Voter authentication in registration systems is largely done via procedural mechanisms. Individual jurisdictions must determine appropriate voter authentication mechanisms. Voters must provide election officials with an authenticator during the registration phase. For election systems using e-mail ballot return, the most likely authenticator is a voter signature. Authenticators must be securely stored by election officials so that it is available to authenticate future correspondence from a voter. Other systems may use passwords, PINs, or digital signatures.

Authentication on election IT systems should be automated and tied to the systems' access control and auditing mechanisms. Systems should identify and authenticate each individual with access to a system, usually through a user name and password. Jurisdictions should develop appropriate policies regarding the use of passwords for authentication, including setting password complexity requirements and expiration times.

***Incident Response (IR):***

Election officials should monitor vital election systems and communications services to ensure they are functioning properly. Officials should monitor audit records of electronic voter registration databases and e-mail servers to verify they are functioning correctly. Officials should also continuously monitor physical access to these systems. To protect against unscheduled service outages and denial of service attacks, administrators should closely monitor the status of Internet connections, and the storage space available on e-mail servers, and implement contingency plans when necessary.

***Maintenance (MA):***

E-mail-based voting systems rely on the software on e-mail servers to assure that election integrity is maintained and that systems remain available to the public. Due to potential software defects in these systems, and the fact that they are connected to the Internet, it is important for

jurisdictions to develop and follow appropriate controls to see that software updates are installed when needed. Because of the threat of malicious code, it is important that these controls ensure that only proper software updates are installed, and that these updates are installed by authorized system administrators.

***Physical Security (PE):***

It is important to limit physical access to election computer systems and voter information. Individuals with physical access to election computer systems may be able to access sensitive records, modify records or software, or cause equipment to fail. Furthermore, individuals with access to storage locations for printed ballots may be able to violate voter privacy or modify votes. Access to areas containing vital election systems should be limited to only those who need access to perform their election-related duties. Access could be limited using locks and/or keycards. Whenever possible, access to these locations should be logged.

***Personnel Security (PS):***

A malicious election official or system administrator may have access to vital election system equipment or information. Jurisdictions should categorize the various roles in their election process according to the level of access to voter information and ballots. Whenever possible, the confidentiality, integrity or availability of the election system should not depend on a single individual. However, that may be infeasible. One jurisdiction may not have multiple employees capable of acting as system administrators for election computer systems. Jurisdictions should take appropriate actions to gain confidence that the administrator will perform his or her duties appropriately. This may include some kind of background screening process.

***System and Communications Protection (SC):***

Sensitive or critical information transmitted over a public communications network typically should have cryptographic protections in order to protect the confidentiality and/or integrity of transmitted data. By itself, e-mail offers little support for cryptographic functionality. However, e-mail based election systems mainly use e-mail to transfer files, such as registration forms or ballots. These files could be cryptographically protected.

Election officials should digitally sign all registration forms and blank ballots before distributing them to voters through e-mail. The Portable Document Format (PDF) files can be digitally signed in some applications that create them. With the correct software, voters' computers will automatically check the digital signature and warn voters of any problems. Such a system would require election officials to create a Digital Signature Standard (DSS) or RSA key pair [23] and apply for a digital certificate from a major certificate vendor. However, only election officials would need to obtain a key pair and certificate.

However, at this time there is no practical way to protect the integrity or confidentiality of e-mails from voters. Thus, returned ballots would be at risk for eavesdropping and modification. Individual jurisdictions must weigh these risks against the convenience of returning ballots via e-mail. S/MIME [22] is a possible solution for digitally signing and encrypting e-mails if voters and elections are able to obtain key pairs and digital certificates. This would require the deployment of a large-scale Public Key Infrastructure.

***System and Information Integrity (SI):***

As previously noted, e-mail voting systems rely on the software running on election computer systems such as e-mail servers and workstations. System administrators should test and monitor their systems to look for defects or vulnerabilities that could prevent votes from being recorded properly, disrupt the elections, or release sensitive information to an attacker. Administrators can check sources, such as the National Vulnerability Database [26], for new security problems with their systems. Furthermore, election computer systems should be protected from various software and network attacks using antivirus software, firewalls and intrusion detection systems.

### 7.5 Web-Based Transmission

Ctrl. No.	Stages			Control Name	Notes	
	RB	BD	BR			
AC-2	X	X	X	ACCOUNT MANAGEMENT	IT systems used to manage registration information and record votes should be protected with access control mechanisms.	
AC-3	X	X	X	ACCESS ENFORCEMENT		
AC-5	X	X	X	SEPARATION OF DUTIES		
AC-6	X	X	X	LEAST PRIVILEGE		
AC-12	X			SESSION TERMINATION		
AU-2			X	AUDITABLE EVENTS	Election systems should include auditing functionality to determine. All computer systems involved in the election process should include system event log functionality. Procedural methods should be used to record manual actions by election officials.	
AU-3			X	CONTENT OF AUDIT RECORDS		
AU-4			X	AUDIT STORAGE CAPACITY		
AU-6			X	AUDIT MONITORING, ANALYSIS, AND REPORTING		
AU-7			X	AUDIT REDUCTION AND REPORT GENERATION		
AU-8			X	TIME STAMPS		
AU-9			X	PROTECTION OF AUDIT INFORMATION		
AU-10			X	NON-REPUDIATION		
CM-2	X		X	BASELINE CONFIGURATION		System administrators should closely monitor the maintenance of vital IT systems to ensure the proper hardware and software updates are performed on such systems.
CM-3	X		X	CONFIGURATION CHANGE CONTROL		
CM-5	X		X	ACCESS RESTRICTIONS FOR CHANGE		
CP-7	X	X	X	ALTERNATE PROCESSING SITE	Officials should prepare a backup telecommunications system in case of an unscheduled outage or attack.	
CP-8	X	X	X	TELECOMMUNICATIONS SERVICES		
IA-1	X		X	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	Officials should develop procedures and implement technical mechanisms to identify voters, election officials and system administrators. Procedures may be used to authenticate voters, while IT systems should include authentication and access control mechanisms.	
IA-2	X		X	USER IDENTIFICATION AND AUTHENTICATION		
IA-4	X		X	IDENTIFIER MANAGEMENT		
IA-5	X		X	AUTHENTICATOR MANAGEMENT		
IA-7	X		X	CRYPTOGRAPHIC MODULE AUTHENTICATION		
IR-4	X	X	X	INCIDENT HANDLING	Officials should monitor their IT systems and communications services for disruptions and possible attacks.	
IR-5	X	X	X	INCIDENT MONITORING		
MA-2	X		X	CONTROLLED MAINTENANCE	System administrators should closely monitor the maintenance of vital IT systems to ensure the proper hardware and software updates are performed on such systems.	
MA-3	X		X	MAINTENANCE TOOLS		
MA-5	X		X	MAINTENANCE PERSONNEL		
PE-2	X	X	X	PHYSICAL ACCESS AUTHORIZATIONS	Officials should control physical access to vital systems and sensitive information. This includes physical access to IT systems and communications equipment.	
PE-3	X	X	X	PHYSICAL ACCESS CONTROL		
PE-4	X		X	ACCESS CONTROL FOR TRANSMISSION MEDIUM		
PE-5			X	ACCESS CONTROL FOR DISPLAY MEDIUM		
PE-6	X		X	MONITORING PHYSICAL ACCESS		
PS-2	X	X	X	POSITION CATEGORIZATION		Screen election employees who will be administering IT systems.
PS-3	X	X	X	PERSONNEL SCREENING		

Ctrl. No.	Stages			Control Name	Notes
	RB	BD	BR		
SC-5	X		X	DENIAL OF SERVICE PROTECTION	Officials must develop protections against denial of service attacks or mitigate the effect with backup procedures. Information sent over telecommunication lines should have integrity and confidentiality protection.
SC-7	X	X	X	BOUNDARY PROTECTION	
SC-8		X	X	TRANSMISSION INTEGRITY	
SC-9	X		X	TRANSMISSION CONFIDENTIALITY	
SC-12	X		X	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
SC-13	X	X	X	USE OF CRYPTOGRAPHY	
SC-14	X	X		PUBLIC ACCESS PROTECTIONS	
SC-20	X	X	X	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	
SC-21	X	X	X	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	
SI-2	X		X	FLAW REMEDIATION	
SI-3	X		X	MALICIOUS CODE PROTECTION	
SI-4	X		X	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES	
SI-5		X	X	SECURITY ALERTS AND ADVISORIES	
SI-7	X		X	SECURITY ALERTS AND ADVISORIES	

***Access Control (AC):***

Web-based registration and voting systems rely on a web server to interact with voters and store vital election information. This system must be protected by strict access control mechanisms. It is likely that some information may be moved to other computer systems. For instance, registration information may be moved to a voter registration database, and tallied votes may be moved to an election management system. Access to information stored on these devices should be limited to employees who need this information to perform election-related duties. Officials should regularly review their access control policies and make appropriate changes as individuals' responsibilities change.

***Audit and Accountability (AU):***

Election computer systems should keep audit records of important events on the system, such as authentication attempts, maintenance and other administrative activities, and voter sessions. The audit records should provide enough information to determine who performed a given action, a description of the action, and the time it took place.

Maintaining the integrity of this information is important, and systems should implement controls which protect audit information from unauthorized access, modification or deletion. Audit records on vital election systems should be digitally signed, preferably using a hardware cryptographic module.

***Configuration Management (CM):***

The integrity of votes and the reliability of the system are dependent on the correctness of software in election web server. System administrators should have a baseline configuration for this system, and access control mechanisms should prevent anyone other than authorized system

administrators from making any changes to this configuration. All changes should be recorded in the audit log for the system.

***Contingency Planning (CP):***

Backup plans and systems should be developed and implemented in the event that Internet service drops due to increased demand, outages, or attacks.

***Identity and Authentication (IA):***

Officials should develop technical and procedural mechanisms to identify all users of the election system, including voters, election officials and system administrators. Initial voter authentication is often done via procedural means. Online voter authentication may need to be done using secret information from the voter. In all cases, each voter must share an authenticator with election officials during the registration phase. Typical authenticators for online systems include passwords, PINs or digital certificates. Authenticators must be securely stored by election officials so that they are available to authenticate future correspondence from a voter.

Authentication on election IT systems should be automated and tied to the systems' access control and auditing mechanisms. Systems should identify and authenticate each individual with access to a system, usually through a user name and password. Jurisdictions should develop appropriate policies regarding the use of passwords for authentication, including setting password complexity requirements and expiration times.

***Incident Response (IR):***

Election officials should monitor vital necessary election systems and communications services to ensure they are functioning properly. Officials should monitor audit records of electronic voter registration databases and election web servers to verify that they are functioning correctly. Officials should also continuously monitor physical access to these systems. To protect against unscheduled service outages and denial of service attacks, administrators should closely monitor the status of Internet connections and implement contingency plans when necessary.

***Maintenance (MA):***

Web-based voting systems rely on the correctness of software to ensure election integrity and availability. Defects and vulnerabilities in voting system software could violate the security goals of the system. System administrators should watch for new vulnerabilities in their systems by monitoring sites such as the National Vulnerability Database [26], and check for updates from software manufacturers. It is important for jurisdictions to develop and follow appropriate controls to see that software updates are installed when needed. Because of the threat of malicious code, it is important that these controls ensure that only proper software updates are installed, and that these updates are installed by authorized system administrators.

***Physical Security (PE):***

It is important to limit physical access to election computer systems and voter information. Individuals with physical access to election computer systems may be able to access sensitive records, modify records or software, or cause equipment to fail. Access to areas containing vital election systems should be limited to only those who need access to perform their election-

related duties. Access could be limited using locks and/or keycards. Whenever possible, access to these locations should be logged.

***Personnel Security (PS):***

A malicious election official or system administrator may have access to vital election system equipment or information. Jurisdictions should categorize the various roles in their election process according to the level of access to voter information and ballots. Whenever possible, the confidentiality, integrity or availability of the election system should not depend on a single individual. However, that may be infeasible. One jurisdiction may not have multiple employees capable of acting as system administrators for election computer systems. Jurisdictions should take appropriate actions to gain confidence that that individual will perform his or her duties appropriately. This may include some kind of background screening process.

***System and Communications Protection (SC):***

Sensitive or critical information transmitted over a public communications network should have cryptographic protections in order to protect the confidentiality and integrity of transmitted data. Web-based election systems should use SSL/TLS to create a secure communications channel between the voter and election web server. Web servers should have a valid SSL certificate from a major certificate vendor. This will allow voters to authenticate the election web server.

For added protection in ballot distribution, election officials should digitally sign all registration forms and blank ballots before posting them on election websites or distributing them to voters online. The Portable Document Format (PDF) files can be digitally signed in some applications that create them. With the correct software, voters' computers will automatically check the digital signature and warn voters of any problems. Such a system would require election officials to create a Digital Signature Standard (DSS) or RSA key pair [23] and apply for a certificate from a major certificate vendor.

***System and Information Integrity (SI):***

As previously noted, web-based election systems rely on the software running on the election web server. This is particularly true for systems which allow for web-based voting. System administrators should test and monitor their systems to look for defects or vulnerabilities in the system that could prevent votes from being recorded properly, disrupt the elections, or release sensitive information to an attacker. Administrators can check sources, such as the National Vulnerability Database, for new security problems with their systems. Furthermore, election computer systems should be protected from various software and network attacks using antivirus software, firewalls and intrusion detection systems.

## 8 Conclusions

This paper discusses the current UOCAVA voting process and provides descriptions of the types of voting materials being exchanged between voters and election officials and the various electronic transmission options available. In addition, this paper describes various threats to those different transmission options and what sorts of security-related controls could be employed to counteract the threats. This section draws upon these threats and controls to arrive at initial conclusions regarding use of these transmissions options with registration and blank ballot requests, delivery of blank ballots, and return of voted ballots. This section also identifies potential next steps; areas of research to pursue in further assisting UOCAVA voters.

### 8.1 Registration and Blank Ballot Request

As noted, all states use the Federal Post Card Application (FPCA) to register military and civilian overseas citizens to register and request ballots. All four transmission options could be used to submit the information required in the FPCA electronically, but use of e-mail and the web present greater challenges at this time.

#### *Use of Telephone and Fax for Registration and Blank Ballot Requests:*

Use of telephone systems by UOCAVA voters to transmit registration and blank ballot requests is similar to use of fax machines in that both systems use the same telephone network infrastructure and therefore share many of the same threats. Many of the threats can be mitigated procedurally. For telephone-based systems, however, certain procedural changes would need to be made in authenticating registration and ballot request information, i.e., a voter would have to prove his or her identity over the phone based on information other than a signature on a fax or postal mail form. If election officials can suitably authenticate voters over the telephone or using fax, these technologies could be used to significantly reduce the delivery times needed to send registration and ballot requests.

#### *Use of E-Mail and Web for Registration and Blank Ballot Requests:*

E-mail and web options for transmitting registration and blank ballot requests currently pose more challenges than for telephone and fax. Network-based attacks could disrupt communications between voters and election officials, or put sensitive personal information from voters at risk of being intercepted. Less sophisticated attacks, such as the spoofing and phishing common in the banking industry, could trick voters into providing their personal information to attackers. These threats are very similar to those faced by many e-commerce applications. Successful use will depend on using similar best practices and techniques as those developed for e-commerce and other internet applications.

### 8.2 Delivery of Blank Ballots

In general, the threats affecting delivery of blank ballots to UOCAVA voters pose less serious challenges than the threats for the return of voted ballots; all four transmission options could be used given careful implementation, including technical and procedural controls.



***Use of Fax for Delivery of Blank Ballots:***

Most threats to faxed delivery of blank ballots can be mitigated procedurally. The remaining threats are both difficult to enact on a large scale and would have a limited effect on the integrity of the election. Faxed delivery of blank ballots could significantly reduce the delivery times compared to postal mail using technology widely deployed today.

***Use of E-mail for Delivery of Blank Ballots:***

E-mail is widely deployed and could significantly reduce delivery times for a large number of voters. However, e-mail delivery of blank ballots relies on various systems that are not under the control of election officials; network-based attacks could interfere with ballots being received properly. E-mail can be read or modified while in transit and can be easily spoofed such that recipients may believe the received ballot is legitimate when it is not. Technical controls, such as digitally signing ballots, can mitigate some of these threats.

***Use of Web for Delivery of Blank Ballots:***

As with e-mail, web-based delivery of blank ballots also relies on various systems that are not under the control of election officials. Network-based attacks pose some threat to these systems, although most can be effectively mitigated using technical controls. Web-based delivery of blank ballots offers some advantages over e-mail in that communications with web servers are more readily protected using widely available security features built into most browsers. While it is difficult to prevent less sophisticated attacks, such as spoofing, the web would offer a convenient and quick ballot distribution method.

### **8.3 Return of Voted Ballots**

The return of voted ballots poses threats that are more serious and challenging than the threats to delivery of blank ballots and registration and ballot request. In particular, election officials must be able to ascertain that an electronically-returned voted ballot has come from a registered voter and that it has not been changed in transit. Because of this and other security-related issues, the threats to the return of voted ballots by e-mail and web are difficult to overcome.

***Use of Telephone for Return of Voted Ballots:***

Voting over the telephone presents a number of security challenges. Election officials would have to use methods other than voter signatures to authenticate voters; these methods, such as use of a PIN, which could be stolen, may present greater risks. Furthermore, a great deal of trust must be placed in the receiving site's equipment to accurately record votes, as there would be no opportunity for voters to directly verify that their ballots have been recorded correctly. The security challenges associated with telephone voting systems are difficult to mitigate using technology that is widely studied and deployed today.

***Use of Fax for Return of Voted Ballots:***

Faxing voted ballots to election officials presents some challenges for maintaining voter privacy and preventing the modification or destruction of voted ballots. Proper procedures may effectively mitigate these threats and reduce the overall risk to a manageable level.

***Use of E-mail for Return of Voted Ballots:***

The use of e-mail to return ballots presents several significant security challenges. Several different computer systems are involved in sending an e-mail from a voter to an election official. Many of these systems, such as the voters' computers and e-mail servers, are outside the control of election officials. Attacks on these systems could violate the privacy of voters, modify ballots, or disrupt communication with election officials. Because other individuals or organizations operate these systems, there is little election officials can do to prevent attacks on these systems. The security challenges associated with e-mail return of voted ballots are difficult to overcome using technology widely deployed today.

***Use of Web for Return of Voted Ballots:***

Casting ballots via the web poses a large number of security challenges that are difficult to overcome. Using this transmission method, voters would log into a web site and submit their selections on a web page. A great deal of trust must be placed in the software on the election server to accurately record votes, as there would be no opportunity for voters to directly verify that their ballots have been recorded correctly.

Furthermore, like e-mail voting systems, a web-based system for casting ballots would rely on computer systems outside the control of election officials. Attacks on these systems, such as voters' computers, could significantly threaten the integrity of elections or the ability of voters to cast ballots. Less sophisticated attacks, such as phishing and spoofing, could trick voters into giving up their voting credentials to an attacker. Such attacks are common in the banking industry, and difficult to defend against. There have been and continue to be significant problems in this industry. Technology that is widely deployed today is not able to mitigate many of the threats to casting ballots via the web.

## ***8.4 Suggested Next Steps***

The threat analysis documented in this paper identifies blank ballot distribution methods as a potential area to immediately improve UOCAVA voting without threatening the security of elections. Fax, e-mail and web-based systems could distribute blank ballots quickly and reliably to voters, significantly reducing the ballot delivery times faced by mailing ballots to voters and improving the UOCAVA voting experience for citizens overseas. In addition, registration and ballot requests can also take advantage of these distribution methods, but there are more threats when handling personal information from voters. Voted ballot return remains a more difficult issue to address, however emerging trends and developments in this area should continue to be studied and monitored.

A number of states already distribute blank ballots via fax or e-mail. However, at this time there are no guidelines that document best practices for fax, e-mail or web-based distribution of ballots. Developing such guidelines could help additional states develop methods for distributing ballots using these transmission methods, and potentially improve the procedures and technical controls already in place in the states currently using these systems.

## References

- [1] FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.
- [2] NIST SP 800-30, Risk Management Guide for Information Systems, July 2002.
- [3] NIST SP 800-53 Rev. 2, Recommended Security Controls for Federal Information Systems, December 2007.
- [4] NIST SP 800-52, Guidelines for the Selection of Use of Transport Layer Security (TLS) Implementations, June 2005.
- [5] NIST SP 800-63-1, Electronic Authentication Guidelines, February 2008 (Draft).
- [6] Voting Assistance Guide, Federal Voting Assistance Program, 2008.
- [7] Dierks, T. and Rescorla, E., *The TLS Protocol Version 1.2*, Internet Engineering Task Force, Request for Comment 5246, August 2008, <http://tools.ietf.org/html/rfc5246>
- [8] ISO 32000-1:2008, Portable Document Format—Part 1: PDF 1.7.
- [9] Klensin, J.. Simple Mail Transfer Protocol, Internet Engineering Task Force, Request for Comment 5321, October 2008, <http://tools.ietf.org/html/rfc5321>
- [10] FIPS 140-3, Security Requirements for Cryptographic Modules, July 2007 (Draft).
- [11] Rockapetris, P., Domain Names- Concepts and Facilities, Internet Engineering Task Force, Request for Comment 1034, October 1987, <http://tools.ietf.org/html/rfc1034>
- [12] NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide, May 2006.
- [13] Vulnerability Note VU#800113, US-CERT, July 2008, <http://www.kb.cert.org/vuls/id/800113>
- [14] Jefferson, D., Rubin, A., Simons, B., Wagner, D., A security analysis of the Secure Electronic Registration and Voting Experiment (SERVE), January 2004, <http://www.servesecurityreport.org>
- [15] Bonsor, K. and Strickland, J. How E-voting Works. <http://people.howstuffworks.com/e-voting4.htm>
- [16] Federal Voting Assistance Program; Voting Over the Internet Pilot Project Assessment Report, Department of Defense, Washington Headquarters Services, June 2001.

- [17] Independent Review Final Report for the Interim Voting Assistance System (IVAS), August 2006.
- [18] Resources for Overseas Citizens and Military Voters. Election Assistance Commission. <http://www.eac.gov/voter/overseas-citizens-and-military-voters>
- [19] Federal Voting Assistance Program, Department of Defense, <http://www.fvap.gov>
- [20] The Uniformed and Overseas Citizens Absentee Voting Act, United States Department of Justice, Civil Rights Division, [http://www.usdoj.gov/crt/voting/misc/activ\\_uoc.php](http://www.usdoj.gov/crt/voting/misc/activ_uoc.php)
- [21] Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), (as modified by the National Defense Authorization Act for FY 2005). <http://www.fvap.gov/resources/media/uocavalaw.pdf>
- [22] S/MIME Working Group, Internet Engineering Task Force, <http://www.imc.org/ietf-smime/>
- [23] FIPS 186-3, Digital Signature Standard (DSS), November 2008 (Draft).
- [24] Military Postal Service Agency, <http://hqdainet.army.mil/mpsa/>
- [25] USPS- Send International Mail, United States Postal Service, <http://www.usps.com/international/sendmail.htm>
- [26] National Vulnerability Database, National Institute of Standards and Technology, <http://nvd.nist.gov/>
- [27] Overseas Vote Foundation, <https://www.overseasvotefoundation.org/>
- [28] Help America Vote Act of 2002, [http://www.fec.gov/hava/law\\_ext.txt](http://www.fec.gov/hava/law_ext.txt)

## Appendix: Acronyms

<b>DNS</b>	Domain Name System
<b>DoD</b>	Department of Defense
<b>EAC</b>	Election Assistance Commission
<b>ETS</b>	Electronic Transmission Service
<b>FIPS</b>	Federal Information Processing Standard
<b>FPCA</b>	Federal Post Card Application
<b>FVAP</b>	Federal Voting Assistance Program
<b>FWAB</b>	Federal Write-In Absentee Ballot
<b>HAVA</b>	Help America Vote Act of 2002
<b>IVAS 2004</b>	Interim Voting Assistance System
<b>IVAS 2006</b>	Integrated Voting Alternative Site
<b>NIST</b>	National Institute of Standards and Technology
<b>PDF</b>	Portable Document Format
<b>PIN</b>	Personal Identification Number
<b>PKI</b>	Public Key Infrastructure
<b>PSTN</b>	Public Switched Telephone Network
<b>SERVE</b>	Secure Electronic Registration and Voting Experiment
<b>S/MIME</b>	Secure/Multipurpose Internet Mail Extensions
<b>SSL</b>	Secure Socket Layer
<b>TLS</b>	Transport Layer Security
<b>UOCAVA</b>	Uniformed and Overseas Citizens Absentee Voting Act
<b>VOI</b>	Voting Over the Internet
<b>VoIP</b>	Voice Over Internet Protocol

## Risks of Internet Voting

Barbara Simons  
[simons@acm.org](mailto:simons@acm.org)  
650-328-8730

All commercially available systems that allow voters to send their voted ballots over the internet, whether via email or a website, are insecure. Furthermore, there are no standards, and there is zero oversight or testing of internet voting systems by any state or federal agency. Typically, the software that runs the systems is secret, so independent computer security experts are unable to analyze the software for bugs, vulnerability risks, privacy violations, and election rigging malware. By allowing voters to use an insecure and unreliable system, we are making them second class citizens and putting our democracy at risk.

Some people think that attaching a copy of one's voted ballot to an email is less problematic than voting at a website, but that is not the case. Because the voter's name is on the email header, the voter is deprived of a secret ballot, opening up voters to the threat of coercion. There is also the increased risk of vote buying/selling.

Email is essentially never encrypted, so ballots sent as email attachments can be read and modified by anyone en route and at the receiving end. In addition, because it is easy to create large number of emails with fake "From:" headers, someone with access to a list of voters could submit thousands of forged ballots.

Another risk is that the voter's computer could be infected with election rigging malware that modifies the vote just before it is sent over the internet. (This is also a risk of web based voting). The voter might think that what she sees on her screen is what goes out over the internet, but that is not necessarily the case. Computers consist of many different components; the screen is only one. There is software between the screen and the link to the internet, and that software could modify a voter's selections without detection.

The threat of criminal malware on a victim's machine is not a theoretical risk. Millions, or even billions, of dollars have been stolen from online bank accounts by malware. The reason we don't hear much about this is that banks quietly cover the losses, because it is cheaper than building new buildings and hiring new tellers. For example, the Zeus Virus, which has stolen vast sums of money from online bank accounts, is so smart that when the victim looks at her online bank statement, it seems correct, even though the money may be in Timbuktu.

Since customized versions of Zeus are available on the black market, and since simply modifying a vote is far easier than stealing large sums of money undetected, the possibility of a Zeus-like virus infecting voters' machines is a real threat.

There are many other risks associated with email voting, including denial of service attacks that overwhelm the election official's machine. In addition, since voted ballots are likely to be sent as pdf attachments, there is the risk that someone wanting to attack the election might infect the election official's machine by sending a fake ballot containing malware in the pdf attachment. (Pdf is known to have security vulnerabilities).

A good thing to keep in mind whenever anyone claims that software is completely secure and reliable is that large software vendors, such as Microsoft and Apple, send out frequent software updates, many of which are to repair security holes in the software. If large wealthy companies with vast numbers of smart programmers are unable to write completely secure and reliable software, why should anyone believe that far smaller voting system vendors can achieve what Microsoft cannot?

In conclusion, because of the risks of software bugs and malware, whenever computers are used in elections, we need to have a way of checking them – ideally a risk-limiting manual post-election ballot audit. But, it is impossible to check the correctness of internet elections, because it is impossible with currently available commercial systems for the voter to verify that the version of an internet ballot received by an election official is identical to the ballot the voter thought she was sending.

An expert on electronic voting, Dr. Barbara Simons was appointed to the Board of Advisors of the U.S. Election Assistance Commission in 2008. She co-authored *Broken Ballots: Will Your Vote Count?* with Prof. Douglas Jones. She was a member of the National Workshop on Internet Voting that was convened at the request of President Clinton and produced a report on Internet Voting in 2001. She also participated on the Security Peer Review Group for the US Department of Defense's Internet voting project (SERVE) and co-authored the report that led to the cancellation of SERVE because of security concerns. Simons co-chaired the Association for Computing Machinery (ACM) study of statewide databases of registered voters, and she co-authored the League of Women Voters report on election auditing.

Simons was President of ACM, the nation's oldest and largest educational and scientific society for computing professionals, from July 1998 until June 2000. She founded ACM's US Public Policy Committee (USACM) in 1993 and served for many years as the Chair or co-Chair of USACM.

In 2005 Simons became the only woman to receive the Distinguished Engineering Alumni Award from the College of Engineering of U.C. Berkeley. She is also a Fellow of ACM and the American Association for the Advancement of Science. She received the Alumna of the Year Award from the Berkeley Computer Science Department, the Distinguished Service Award from Computing Research Association, the Making a Difference Award from ACM's Special Interest Group on Computing and Society, the Norbert Wiener Award from Computer Professionals for Social Responsibility, the Outstanding Contribution Award from ACM, and the Pioneer Award from the Electronic Frontier Foundation. She was selected by C|NET as one of its 26 Internet "Visionaries" and by Open Computing as one of the "Top 100 Women in Computing." Science Magazine featured her in a special edition on women in science.

Simons served on the President's Export Council's Subcommittee on Encryption and on the Information Technology-Sector of the President's Council on the Year 2000 Conversion. She is the Chair of the Board of Directors of Verified Voting, and has also been on the boards of the U. C. Berkeley Engineering Fund, the Electronic Privacy Information Center, Public Knowledge, and the Oxford Internet Institute, as well as the Advisory Council of the Public Interest Registry's ORG. She has testified before federal and state legislatures and at government sponsored hearings. She was runner-up in the first election for the North America seat on the ICANN Board.

Simons co-founded the Reentry Program for Women and Minorities in the U.C. Berkeley Computer Science Department. She is on the Boards of the Coalition to Diversify Computing and the Berkeley Foundation for Opportunities in Information Technology, groups devoted to increasing participation in computer science of women and underrepresented minorities.

Simons earned her Ph.D. in computer science from the University of California, Berkeley. Her dissertation solved a major open problem in scheduling theory. In 1980, she became a Research Staff Member at IBM's San Jose Research Center (now Almaden). In 1992, she joined IBM's Applications Development Technology Institute as a Senior Programmer and subsequently served as Senior Technology Advisor for IBM Global Services. Her main areas of research have been compiler optimization, algorithm analysis and design, and scheduling theory. Her work on clock synchronization won an IBM Research Division Award. She holds several patents and has authored or co-authored two books and numerous technical papers. She is retired from IBM Research.

# Hazards of Email Voting

David Jefferson

Lawrence Livermore National Laboratory

[drjefferson@gmail.com](mailto:drjefferson@gmail.com)

925-989-3701

March, 2015

From a security point of view email voting is about the worst form of voting ever proposed. It is easy for many parties to read or modify ballots *while in transit* from the voter to election officials. It is also easy to simply block selected ballots from being delivered. Such attacks can be *automated* to affect a large number of votes, and can be perpetrated remotely, by anyone on Earth, including criminal syndicates, domestic partisans, or foreign intelligence agencies. Neither the voter nor the election officials can detect such attacks, let alone prevent or correct for them. Sending ballots by email is as dumb as taping a \$100 bill to a postcard and expecting it to be delivered safely. Basically, it is naïve and irresponsible to send any kind of secure or confidential document by ordinary email.

In more detail, here are the technical facts.

**1) Email uses no encryption:** Ordinary civilian email such as voters would use from their home PCs or mobile devices is not end-to-end encrypted. The headers, the text, and the attachments (i.e. the ballot) are all sent entirely in the clear, and there is no good way around this. It makes email less secure than a postcard. This lack of encryption has many disastrous security consequences.

- **Ballots can be modified in flight to vote an attacker's choices:** Because it is unencrypted an email containing a voted ballot can be modified arbitrarily or substituted on the fly by malicious code in the voter's own infected computer or mobile device, or in the voter's home router, or by malicious logic in any router or mail forwarding server along the path from the voter to the mailbox of election officials. Any IT person in charge of those routers or servers can do this, as well as any remote attacker from anywhere in the world who chooses to hack one or more of systems. This has actually been demonstrated (not that it was necessary) by Joe Kiniry of Galois. There is no fundamental protection against this at all, and no way to detect that it has happened. Furthermore it is easy for an attacker to select, out of the millions of email messages being transmitted, exactly those that contain ballots, because they (and only they) are sent to the official email address(es) used for collecting ballots.
- **Ballots can be selectively dropped in flight:** Lazy attackers don't have to go to the trouble to actually modify ballots in flight to affect the election outcome. They may simply throw away email messages that contain ballots with votes that they don't like, and let through emailed ballots they do like.



Again, neither the voter nor the intended receiver will know, at least until it is too late.

- **Ballots can be read or copied in flight:** Even if not modified or dropped in flight, email containing ballots can be read or copied by anyone with control of a router or email forwarding server through which the ballot it passes. There are several serious consequences of this:
  - (a) Vote privacy is completely lost, because the voter's name and email address are attached to the voted ballot.
  - (b) The loss of vote privacy enables large scale vote buying and selling schemes, or coercion.
  - (c) Many people have their email service through their employer's infrastructure, and employers have the legal right to inspect and archive all email sent to or from employees through company infrastructure. This includes military personnel who would vote in the clear through military networks.
  - (d) Emailed ballots can be copied to third parties in flight. This would be valuable for domestic political operatives who want to know exactly who is voting for what or who want count the votes early to see how to invest their campaign resources during the last days of a campaign while balloting is in progress.

**2) Email headers are totally forgeable and modifiable:** The From and Date headers on email are not encrypted, and hence are totally forgeable or modifiable in flight. It is easy to send email that appears to come from someone else. (Spammers do it all the time.) And it is easy to modify the dates on email to make it appear that emailed ballots sent after the close of the election were sent earlier (and thus should be counted in states where the sending date is the criterion used).

**3) Email offers no voter authentication:** There is no way to verify the authenticity of an email, or that it actually comes from the voter it purports to. We have no national ID, nor any fingerprint or other technical means of authenticating email. Not only is the From header completely forgeable, but even if the voter is required to provide some additional private information (such as birthdate, SSN, driver's license number, or password of some kind) that is a very weak kind of authentication. Hundreds of millions of people's private information has been compromised already via many commercial cyber attacks that have made news in recent years. And if private information is sent along with the ballot, it is sent in the clear (unencrypted) like the rest of the email, so an attacker can collect that private information while also substituting a ballot containing votes that the attacker likes.

**4) Email is only a best efforts delivery service:** Email is normally delivered in minutes, but this is not guaranteed. Email is a "best efforts" delivery service. Because ISPs do not charge for email, they feel no obligation to offer any speed

guarantees. Email with attachments (e.g. a ballot) is often delivered much more slowly than email that contains only text. We are all familiar with cases where email has been delayed by hours or even days, a hazard that could effectively disenfranchise voters who sent the ballot by email in the last hours of Election Day.

**5) PDF can be used to deliver malware to the server:** Most email voting systems require the ballot and the user's identification to be in the form of PDF attachments to the email message. However, PDF is a notoriously dangerous file type because specially constructed PDF files can be used to deliver malware to whoever receives and opens it. An attacker could create a malicious PDF file that looks like a benign ballot but contains malware. When it reaches the election server it could introduce a backdoor for the attackers to gain control of the election server.

**6) Email is subject to all the other generic attacks the Internet is vulnerable to:** The above problems are just those specific to *email* voting. But there are generic attacks on Internet traffic of *all* kinds that affect email as well as all other kinds of communication, e.g. the web. These include:

- *Denial of service attacks*, which can so clog a server with traffic that nothing can get through for several hours until defensive efforts can be ramped up. But several hours on Election Day can be the difference between thousands of ballots arriving on time vs. arriving too late to be legally counted. These attacks are notoriously easy to perform in a large variety of distinct ways, and there are whole dark businesses on the Internet that will conduct such an attack for you (for a price) if you don't want to do it yourself.
- *Server penetration attacks*, in which the attacker directly attacks the server that collects the emailed ballots and modifies, copies, or deletes ballots as the attacker desires.
- *DNS poisoning attacks*, which can cause ballots to be transmitted to the wrong place, so they never reach the election server at all.
- And there are many others.

## Bio for David Jefferson

Dr. David Jefferson is an internationally recognized expert on voting systems and election technology. He has been a pioneer in research at the intersection of computing, the Internet, and elections for 20 years, and has been an advisor to five successive Secretaries of State of California on technology-related issues.

In 1994, in the earliest years of the web, Jefferson developed the California Election Server in cooperation with Acting California Secretary of State Tony Miller, Digital Equipment Corporation, and the California Voter Foundation. This was the first web server anywhere to provide online voter information on candidates and issues, as well as live election returns, setting a world traffic record of 1 million page hits in 24-hours. In 1999 Jefferson chaired the technical committee of Secretary of State Bill Jones' Task Force on Internet Voting, whose report was the first major study of that subject. In 2003, he was a member of the Secretary of State Kevin Shelley's Ad Hoc Task Force on Touchscreen Voting, whose recommendations led eventually to voter verified paper audit trails for electronic voting machines in California. He subsequently chaired the Voting Systems Technology Assessment and Advisory Board under Secretary of State Bruce McPherson. In that capacity he led and coauthored half a dozen detailed technical studies on reliability and security problems in particular voting systems. In 2007 under Secretary of State Debra Bowen he chaired the Post-Election Audit Standards Working Group that worked in parallel with the Top to Bottom Review to produce the first government-sponsored report on the subject of post-election auditing ([www.sos.ca.gov/elections/elections\\_peas.htm](http://www.sos.ca.gov/elections/elections_peas.htm)).

In 2004 he was coauthor of the SERVE Security Report, which detailed major security vulnerabilities in the DoD's proposed SERVE Internet voting system, which led to the cancellation of the program ([www.servesecurityreport.org](http://www.servesecurityreport.org)).

Jefferson has been an invited speaker on election technology issues at the annual conferences of IACREOT (International Association of Clerks, Records, Election Officials and Treasurers), NASED (National Association of State Election Directors), and the Election Center, as well as at universities such as Stanford, M.I.T., U.C. Berkeley, U. T. Austin, Evergreen College, U.C. Irvine, University of Calgary, and University of Massachusetts, and numerous other venues. He has also consulted with numerous agencies and states on the subject of voting security, including the FEC and the Department of Defense.

In 1980 Jefferson received a Ph.D. in computer science from Carnegie-Mellon University. From 1980 to 1994 he was a computer science professor, first at USC and then at UCLA, where he conducted research in parallel computation, simulation, and genetic algorithms. In 1990 he received an R&D 100 Award for leading one of the top 100 R&D projects in the United States, and in 1996 he received a James Madison Freedom of Information Award for his work on bringing nonpartisan election information to the web.

Jefferson is a member of the boards of directors of the California Voter Foundation ([www.calvoter.org](http://www.calvoter.org)) and of Verified Voting ([www.verifiedvoting.org](http://www.verifiedvoting.org)), two nonprofit, nonpartisan organizations devoted to promoting open, secure election technology. In 2009 served as the Co-Chair for the EVT/WOTE '09 conference – the primary academic voting technology and security conference in the U.S. ([www.usenix.org/event/evtvote09](http://www.usenix.org/event/evtvote09)).

Jefferson is well known among computer scientists for the co-invention of the Time Warp method of parallel discrete event simulation. He is currently at Lawrence Livermore National Laboratory, where he leads research in discrete event simulation for various national security applications. He and his colleagues recently set a world record for extreme scale and sustained speed of a discrete event simulation using LLNL's Blue Gene/Q supercomputer *Sequoia*.

## I D C T E C H N O L O G Y S P O T L I G H T

---

# Dynamic Authentication: Smarter Security to Protect User Authentication

September 2014

Adapted from *Worldwide Identity and Access Management 2013–2017 Forecast* by Sally Hudson, IDC #241685

Sponsored by SecureAuth

---

### Introduction: The Need for Dynamic Authentication

User authentication has been a thorn in the side of anybody who has ever tried to gain access to an application and forgotten his/her password — that is to say, everyone. Nevertheless, authentication is a crucial element of technology risk management because it provides the key mechanism for "letting the good guys in" by linking users to their online accounts and creating a delineation between legitimate users and malicious hackers.

To maximize the value of technology resources, security professionals must seek out authentication means that perform the best by allowing the highest number of legitimate users to access systems while denying the highest number of illegitimate users (system attackers), all for the lowest possible economic costs.

Providing a more dynamic mechanism for authentication creates an opportunity for creative ways to introduce and require various authentication factors based on some notion of risk. With these newer approaches, we can increase the effectiveness of authentication by reducing false positives and false negatives.

Adaptive, risk-based, context-based authentication techniques are well-known in consumer banking environments and online business sites but are just now gaining interest within enterprises as they consider ways to evolve their control environments to meet the needs of newer cloud and mobile IT architectures.

### Technology Trends

Several key technology trends are driving the need for organizations to reevaluate their authentication strategies, including:

- **More distributed architectures for applications.** Enterprises are constantly creating more flexible and "loosely coupled" architectures so that individual components can be accessed, replaced, updated, and managed more easily.
- **Access to APIs and mashups.** Outside of applications, links to external services are becoming much more common as collaborative environments arise and new capabilities are added to the Internet.

- **Continued recognition of the value of mobility.** Adoption rates and usage of mobile devices continue to increase, making the platform more useful while recognizing that connectivity is not continuous. This value also drives the proliferation of multiple mobile devices per individual.
- **Bring your own x.** Organizations are increasingly allowing personal or unmanaged devices onto their networks.

These trends make secure authentication generally more difficult for yet often even more important to enterprises.

## Authentication Challenges with New Tech Architectures

When taking technology trends into account, organizations must consider how the authentication process changes along with them:

- The credentials may not be issued by the resource owners. Attempts at spoofing users or accounts may have a higher probability of success.
- The credentials may be used for longer periods of time — sometimes even while disconnected from the network — and thus create a staleness that reduces or dilutes the strength of the authentication mechanism.
- The strength of the credentials may not align well with the sensitivity of the assets or resources being requested.

## Threat Trends

The thing that makes technology risk management unique is the introduction of the "intelligent adversary." Scenarios are created that result in unwanted outcomes (incidents and breaches), and attackers can adapt their techniques to create an opportunity for more success.

Along with changes being made to IT architectures, enterprises must deal with evolving threats:

- Malicious actors are increasingly gaining opportunities to attack and compromise systems by capitalizing on new technology trends and authentication challenges.
- Outsiders are "becoming" insiders as they find more opportunities and ways to steal credentials.
- Privilege escalation is the practice of using an account with lower privileges to compromise the system in a way that elevates the privilege level of that account or another account.
- Man-in-the-middle (MITM) attacks, where the attacker is positioned on a device that can intercept and modify requests and responses, are becoming more common.

## Authentication Trends

The final piece of an authentication strategy is to consider trends in how newer solutions are architected. The days of legacy "two-factor" authentication have given way to solutions that align more closely with the tech architectures. These trends include:

- "Cache and carry" credentials, which provide a means for leveraging mobile devices in the authentication process (It is common for authentication information to be maintained on the phone as part of the application architecture. In addition, the phones can be used to provide data that can be leveraged for authentication solutions.)

- Federation and delegation standards, which are extremely popular with enterprise solutions (These capabilities extend the reach of authentication operations to external applications or systems.)
- Multifactor, multiform, multiframe authentication solutions, which are becoming commoditized as the need for custom hardware is lessening (Many different options exist to negotiate an authentication operation.)

If not handled correctly, trends toward increased lifetime of sessions and increased authentication scope could be worrisome. However, as these authentication trends develop, newer architectures also provide for an authentication operation to occur not only at the beginning of a session but also at key points or for key transactions during the session.

### **Solution: Dynamic Authentication**

In some respects, the authentication trends lean toward more convenient yet possibly weaker methods. And while it is important to recognize the importance of convenience to users, the increasing threat requires stronger, not weaker, processes. The way to strengthen the process is through more appropriate authentication requirements at more appropriate times.

IDC defines "dynamic authentication" as the evaluation of information offered to prove an identity after a user session has been initiated. The key to dynamic authentication, essentially, is to make it harder for a user to verify his/her identity in circumstances that either are or appear to be higher risk. The goal is to be more effective while providing a productive environment for users.

The tools for dynamic authentication have been available for some time; the circumstances and trends described previously make it more beneficial to implement them for traditional enterprise authentication.

### ***Standard Authentication Revisited***

Authentication has traditionally leveraged the provision of three types of evidence, or factors, during an authentication process:

- Something you know — passwords, mostly, but can be related to anything that is a secret shared between the user and the resources being accessed
- Something you have — various tokens that are issued where ownership can be used as proof of identity
- Something you are — biometric information that may be compared with "known good" information collected at an earlier time

Each of these factors may still be used during dynamic authentication, often in various combinations. For example, it is common for cloud applications to send an SMS text message (a shared secret, something you know) dynamically to a cell phone on file (something you have) to verify ownership of an account for certain types of changes to be made.

The differences between traditional authentication and dynamic authentication lie in the reason why authentication is being requested. Authentication traditionally happens at the beginning of a session between a user and an application or a service. Now, service providers may request authentication at various points during a session, for various reasons.

### ***Information: Attributes and Activities***

Various types of information may be leveraged to help make the decision to trigger some form of authentication action. IDC has classified four categories of evidentiary information that may be collected, managed, and used during a dynamic authentication process:

- Static device-based attributes — information about a device that rarely/never changes (for the device) that can be used to fingerprint devices for comparison and tracking over time
- Ephemeral device-based attributes — information collected from a device that generally changes or can change, including geo-location and browser/device type
- Activity-based attributes — information such as time, functional operation, and resources used that can be evaluated in various ways to determine whether further authentication is required
- Resource-oriented attributes — information about a resource, regardless of who the user is, that may be leveraged to trigger a dynamic authentication operation

Collecting this information and making it available for analysis is only the beginning of dynamic authentication. More importantly, the information must be evaluated.

### ***Evaluation Methods***

As with any inline control, dynamic authentication must incorporate some test to determine when it is necessary. The most popular tests are as follows:

- Evaluate reputation — comparing information about a session with a set of "known bad" (or sometimes "known good") sources that track IP addresses, email accounts, resource names, and other attributes for threat intelligence purposes (This approach is often referred to as blacklisting or whitelisting.)
- Identify known bad actions/sequences of actions — comparing the activity being performed in a session with previously identified universally bad behavior (commonly referred to as signatures)
- Identify deterministic differences — comparing the static attributes identified during a session, such as device ID or device type, with some set of known static attributes
- Identify (population) anomalous activity — comparing existing session activity with the historical activity of the entire user population to identify anomalous behavior
- Identify anomalous user activity — comparing the current activity of a user with the previous activity of the same user in search of anomalies

The latest generation of solutions not only will perform many of the tests listed previously but also will frequently create aggregated risk scores that can be used for threshold analysis. In addition to the techniques listed, higher-order analytical techniques — essentially "big data" algorithms — are being applied to the continuous identity verification challenge.

### ***Dynamic Response Methods***

The final step in dynamic authentication is to respond to the tests and techniques described. At a basic level, any test that generates a concern about identity can be responded to with a request to reauthenticate. In addition, a solution will have capabilities to require "step-up" authentication and request more proof of identity — one or more of the traditional factors involved.



## Benefits

There is good reason for dynamic authentication as the authentication process itself can be very cumbersome to end users. As always, the value proposition revolves around efficiency and effectiveness:

- **Provide fewer false positives.** The most onerous part of a user's experience comes during failed log-in attempts for legitimate users. These false positives not only are a burden to the user but also often require an expensive call to a help desk. In addition, the reset process itself may be compromised. Dynamic authentication allows users to authenticate initially in a simple way yet retains the right and opportunity to increase the proof under appropriate, higher-risk circumstances such as anomalous behavior or when accessing sensitive resources.
- **Provide fewer false negatives.** As the scope of the initial authentication action increases across resources, the risk is likely to increase along with it. Dynamic authentication solutions can create opportunities for reauthentication during a session and thus reduce the chance that a user account will be successfully compromised.
- **Lower costs.** Assuming that the false positives and negatives are reduced, a dynamic authentication solution should reduce the costs associated with password resets and actual incidents.

Ultimately, the goal of the dynamic authentication solution is to create a better customer experience while maintaining the balance between reducing costs and reducing risks.

## Considering SecureAuth's IdP v8.0

SecureAuth, an information security company based in Irvine, California, has released the latest version of its flagship product, SecureAuth IdP. The new release is designed to improve the security of access control with an enhanced risk analysis feature. IdP v8.0's analysis includes four factors that work together to mitigate attacks and to automate an organization's desired response:

- **IP Address examination** immediately determines whether the user is working from a recognized IP address and can compare this address with an established whitelist or blacklist.
- **IP Reputation** utilizes a real-time threat intelligence service powered by Norse DarkViking. User IP addresses are examined and a risk score is returned based on various criteria. Administrators can set risk thresholds, which determine what the acceptable risk should be for a particular application. The "presets" are low, medium, high, and extreme, but an advanced setting can be used to customize the risk score.
- **Group Membership** analyzes the user's existing group membership information so that administrators can allow or deny access to an application based on the group list provided.
- **Geo-location/Geo-velocity** uses the IP address to calculate the user's current coordinates and then compare the time and location of the current log-in attempt with the time and location of the previous attempt. Based on the acceptable velocity that the administrator defines, users who normally log in from Southern California can be prevented access from Russia one hour later.

Utilizing a risk score composed of over 40 different threat detections, IP restrictions, group membership, and geo-location/geo-velocity, IdP 8.0 analyzes users and devices to recognize anomalies within the access control workflow. Organizations can then choose how to handle the assessment with a hard stop, a redirection, or a step-up authentication requirement, which occurs automatically.

As noted previously, SecureAuth has partnered with Norse Corporation, integrating live threat intelligence technology into IdP 8.0. The Norse DarkViking threat intelligence tool provides a real-time, continuously updated feed that helps organizations identify attackers — especially from the darknets — that other systems miss. SecureAuth's strategy is to apply this depth of threat intelligence to the user authentication process to ensure that only authorized users gain access. The company expects that future SecureAuth solutions will detect and prevent cyberthreats and identify attackers at the authentication level, before harm can be done.

### **Challenges**

While there is great promise for dynamic authentication overall, the risk-based or higher-order techniques are unproven. This may build a more skeptical market, require more resources to test, and extend the sales cycles of vendors in the space.

There are a number of vendors in this area and the closely related Web-fraud market, each with its own take on the "best" solution. SecureAuth's competition will continue to intensify as the market develops and winners are chosen by customers.

Also, many customers will not have a strong understanding of the user environment and will be concerned about complexity. SecureAuth must ensure that the solution is implemented in a way that provides value early in its deployment.

### **Conclusion**

It's clear that dynamic authentication is gaining steam. We can apply techniques already in use for consumer banking and other high-risk transactions — and both technology risk managers and users win. To the extent that SecureAuth can successfully address the challenges described in this paper, the company is well-positioned in this strategically important market.

---

#### ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

#### COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the IDC Custom Solutions information line at 508-988-7610 or [gms@idc.com](mailto:gms@idc.com). Translation and/or localization of this document require an additional license from IDC.

For more information on IDC, visit [www.idc.com](http://www.idc.com). For more information on IDC Custom Solutions, visit [http://www.idc.com/prodserv/custom\\_solutions/index.jsp](http://www.idc.com/prodserv/custom_solutions/index.jsp).

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 [www.idc.com](http://www.idc.com)