OFFICE OF THE GOVERNOR

Governor's Office of Information Technology

RULES IN SUPPORT OF THE COLORADO INFORMATION SECURITY ACT

8 CCR 1501-5

[Editor's Notes follow the text of the rules at the end of this CCR Document.]

R 24-37.5-403(2)(b) Authority

The authority to promulgate rules is 24-37.5-403(2)(b), CRS and the State Administrative Procedures Act, section 24-4-101 et seq. (the "APA"), CRS and the Information Security Act, sections 24-37.5-401 through 405 (the "Act"), CRS

R 24-37.5-403.2 Scope and Purpose

A. This rule shall govern every public agency ("agency" or "agencies") as defined in CRS 24-37.5-402(9). "public agency" means every state office, whether executive or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

B. This regulation does not apply to state-supported institutions of higher education.

R 24-37.5-403.3 Applicability

The provisions of this section shall be applicable to all public agencies that manage and administer IT systems intended to store, process, or transmit data.

R 24-37.5-403.4 Definitions

ACSP – Agency Cyber Security Plan.

Access Control - Access controls are typically logical controls designed into the hardware and software of a computing system. Identification is accomplished both under program control and by using physical controls.

Agency Chief Information Officer (Agency CIO) - A role delegated to a knowledgeable employee within an nonconsolidated agency, responsible for approving the agency cyber security plan.

CCSP – Colorado Cyber Security Program.

Change Control - Process for controlling modifications to hardware, firmware, software and documentation to ensure the information system is consistently available to users and the system and data it contains are protected from improper modification before, during, and after the system implementation.

Configuration Management - Process for consciously configuring hardware, firmware, software, and documentation to ensure the information system is protected against improper use or unintended failure before, during and after system implementation.

Consolidated Agency or Agencies – All public agencies whose information technology and information security responsibilities were consolidated within the Governor's Office of Information Technology.

Cyber Security Incident - Any event, suspected event, condition, and/or vulnerability that could pose a threat to the confidentiality, integrity, or availability of systems, applications or data.

ECSP – Enterprise Cyber Security Plan -The consolidated, integrated cyber security plan created by the Governor's Office of Information Security for all consolidated agencies in compliance with these rules.

Enclave - A security Enclave is a logical boundary surrounding all resources that are controlled and protected. The protected resources are called a domain (or enclave or protected subnetwork). There may be overlapping domains of varying protection, so that the most sensitive resources are in the innermost domain, which is the best protected. Protecting the security perimeter may be physical controls, identification and authentication, encryption, and other forms of access control.

Event - An event is any observable security occurrence in a system and/or network.

Firewall - A method of guarding a private network by analyzing the data and applying access control rules.

General Support System - An interconnected information resource under the same direct management control that shares common functionality.

Information Security Officer (ISO) – A role delegated to a knowledgeable employee or contractor within an agency, responsible for supporting the agency cyber security plan.

Information Security Operations Center (ISOC) – Statewide cyber security monitoring and analysis team responsible for security operations for shared state services.

Individual Accountability - Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Intrusion Detection - Intrusion detection is the process of identifying attempts to penetrate a system and gain unauthorized access.

Major Application or Major Information System - An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application.

Non-Consolidated Agency or Agencies - Those public agencies whose information technology and information security responsibilities were not consolidated within the Governor's Office of Information Technology but are required to comply with these rules.

Patch – Otherwise known as a software update. A patch is a piece of code that is added to software in order to fix a bug or problem. It is used most frequently as a temporary correction between two version releases.

POA&M - Plan of Action and Milestones: consists of agency remediation plans to close compliance gaps and mitigate known risks to communications and information resources.

Remote Access - Remote access is the ability to get access to a computer or a network from a remote distance. In corporations, people at branch offices, telecommuters, and people who are traveling may need access to the corporation's network.

Risk - The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Assessment – A process used to identify and evaluate risks and their potential effects.

Risk Management - The ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Security Incident - Means an accidental or deliberate event that results in or constitutes an imminent threat of unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources.

SDLC - System Development Life Cycle: a process that each agency deploys to manage the acquisition, development, deployment, maintenance and replacement of systems.

State CIO – The person responsible for overseeing the operations of the Governor's Office of Information Technology and for delivering information technology, including information security, services to consolidated agencies within the executive branch (as defined in 24-37.5-102(1))

R 24-37.5-403.5 Rule

A. Cyber Security Planning: It is the policy of State of Colorado to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of sensitive electronic information assets.

1. Each public agency in the State of Colorado shall maintain a Cyber Security Plan to control risks associated with access, use, storage and sharing of sensitive citizen and State electronic information, and document the program details in an Agency Cyber Security Plan (ACSP) for non-consolidated agencies or an Enterprise Cyber Security Plan (ECSP) for consolidated agencies. An Agency Cyber Security Plan or an Enterprise Cyber Security Plan shall include the following sections, at a minimum:

a. Public agency Mission Objectives

(1) Mission Statement: *Summarize or insert the Public Agency/Agencies Mission Statement(s)*.

(2) Concept of Operations: *Describe the operational goals of the Cyber Security Program, and the conceptual functions that are implemented to achieve these goals*.

(3) Roles and Responsibilities: *Identify responsibilities for implementing, monitoring, and managing the Cyber Security Program, specifically including the responsibilities of the Executive Director, Agency ISO, Agency CIO, State Chief Information Officer, State Chief Information Security Officer (CISO), Security Staff, Agency IT staff, Agency Human Resources staff, and Agency staff*.

b. Information Technology Environment

(1) Network Environment, Enclaves, and Perimeters: *Describe the current network environment in detail, including characterizing of network*

segments into Security Enclaves, and identify the perimeters of each Security Enclave.

(2) Critical Systems: *List Agency critical systems by name, function, and the network segments they reside on.*

(3) General Support Systems: *Define general support systems as they pertain to the environment (e.g., Active Directory Domains/Forests, NIS+ domains, or Email systems)*.

c. Risk Management

(1) Risk Assessment Methodology: *Describe the methodologies used for formal and informal System-level and Agency-wide Risk Assessments, and the process for initiating a Risk Assessment, mitigating unacceptable risk, approving residual risk, and updating existing Risk Acceptance. Include the identification of the individual responsible for accepting residual risk*.

(2) Risk Assessment Responsibilities: *Identify any responsibilities in the Risk Management function that are outside the scope of the Roles and Responsibilities section of the ACSP/ECSP*.

(3) Risk Assessment Frequency: *Identify the maximum length of time between System-level and Agency-wide Risk Assessments*.

(4) Project Lifecycle: *Describe how the Risk Management strategy is integrated into System, Network, and Application engineering project lifecycles, specifically identifying control points that trigger Risk Management activities*.

(5) Vendor Management: *Describe the role of Risk Management in the assessment, selection, and management of IT service providers or vendors*.

d. Security Program

(1) Network Operations: *Describe standards for Network Operations as they pertain to Network Access Controls, Perimeter Security, Network Administration, Monitoring and Reporting, and Network Device Inventory*.

(2) System and Application Security: *Describe standards for System and Application Security as they pertain to Access Controls, System Administration and Engineering, Change Control and Configuration Management, Patch Management, Malicious Code, Monitoring and Reporting, and System Backups*.

(3) Access Controls: *Describe standards for Hiring, Termination, and Transfer of staff and how it relates to user account administration. Include a description of the process used to approve system access requests based on need-to-know and describe how "least-privilege" is achieved in the environment*.

(4) Change Control and Configuration Management: *Describe the components of Change Control and describe the integration of the Cyber Security Program as it relates to Change Control. Describe the minimum*

standards for configuration management as it relates to System, Network and Application engineering.

(5) Physical Security: *Describe the requirements for physically securing the Agency's Sensitive Areas*.

(6) Data Handling and Disposal: *Describe the procedures used to achieve the goals of the CCSP Data Handling and Disposal Policy*.

(7) Personnel Security: *Describe the process for and frequency of performing background checks on IT and Security staff*.

(8) Acceptable Use: *Identify the required elements of the Agency's Acceptable Use Policy and the responsibilities for ensuring all users have received and acknowledged it*.

e. Incident Warning, Advisory, and Response

(1) Cyber Security Warnings and Advisories: *Describe the process for evaluating both Vendor and ISOC-issued Cyber Security Warnings, Patch Announcements, and Security Advisories and describe the standard for recording the response, including time frame for response, acceptable responses, and responsibilities for evaluating the Warning or Advisory*.

(2) Cyber Security Incident Response Plan Summary: *Provide a summary of the Agency's Incident Response Plan, including naming the individual(s) who lead the team*.

f. Training and Awareness

(1) Methodology: *Describe the methods for delivering Initial and Refresher Training to staff. Describe any differing levels of Cyber Security Training that are provided to individuals holding specific job responsibilities (end user, system administrator, security administrator, and managers), if applicable. Describe methods of providing periodic security awareness notices to Agency staff, and the responsibilities for issuing these notices*.

(2) Frequency: *Identify the required frequency for Refresher Training and Security Awareness Notices*.

(3) Content Updates: *Identify the role or individual responsible for providing updated training content and awareness notices*.

g. Self-Assessment: *Describe the required elements of the Cyber Security Self-Assessment Process, the roles and responsibilities in carrying out the Self-Assessment, and the integration of the Self-Assessment results into a program improvement process.*

h. Metrics and Reporting: *Describe the types of metrics that are being collected by the Agency Cyber Security Program and how they are being used to evaluate the effectiveness of the Program.*

i. Plan Approval and Maintenance: *Identify the frequency of the ACSP/ECSP updates and the roles that are responsible for making and approving the updates. The*

Agency Executive Director and the Agency CIO are required approval authorities for the ACSP. The State Chief Information Officer and the State Chief Information Security Officer are the required approval authorities for the ECSP.

2. To carry out the ACSP, the public agency shall delegate the position of Information Security Officer to an agency staff member or contractor who has appropriate Cyber Security experience and public agency IT environment knowledge. The Chief Information Security Officer shall be responsible for carrying out the ECSP.

3. Annually, on or before July 15 th of each year, each public agency shall submit their ACSP to the State CISO for his or her review. The State CISO shall review and approve, conditionally approve, or disapprove each ACSP based on evaluation of the Plan and supporting documentation. Annually, on or before July 15 th of each year, the State Chief Information Security Officer shall submit the ECSP to the State Chief Information Officer for review and approval

   a. Each non-consolidated agency shall submit an approval package to the CISO, consisting of:

      (1) Cover letter requesting ACSP approval

      (2) Agency Cyber Security Plan (ACSP)

      (3) Agency-wide Risk Assessment

      (4) Agency Disaster Recovery Plan Summary

      (5) Agency Disaster Recovery Plan test results

      (6) Agency Self-Assessment results

      (7) Agency Cyber Security Plan of Action and Milestones (POA&M)

      Documents numbered 2 through 7, above, are not public records pursuant to Sections 24-72-202 (6) (b) (X) CRS and 24-72-202 (6) (b) (XII) CRS. Each such document and any supporting materials shall be labeled "Confidential" and "Not a Public Record."

   b. The cover letter is an assertion to be signed by the Executive Director that either states that the public agency is compliant with the Colorado Cyber Security Program or that the Agency Cyber Security Plan of Action and Milestones contains active initiatives that will bring the public agency into compliance.

   c. For the ECSP, *the CISO shall submit the following to the CIO:*

      (1) Cover letter requesting ECSP approval

      (2) Enterprise Cyber Security Plan (ECSP)

      (3) Enterprise-wide Risk Assessment

      (4) Enterprise Disaster Recovery Plan Summary

      (5) Enterprise Disaster Recovery Plan test results

(6) Enterprise Self-Assessment results

(7) Enterprise Cyber Security Plan of Actions and Milestones (POA&M)

Documents numbered 2 through 7, above, are not public records pursuant to Sections 24-72-202 (6) (b) (X) CRS and 24-72-202 (6) (b) (XII) CRS. Each such document and any supporting materials shall be labeled "Confidential" and "Not a Public Record."

The cover letter for the ECSP is an assertion to be signed by the State CISO that either states that the enterprise is compliant with the Colorado Cyber Security Program or that Enterprise Cyber Security Plan of Action and Milestones contains active initiatives that will bring the enterprise into compliance.

Editor's Notes

History

Entire rule eff. 12/30/2013.