Cyber Security Services (CSS)

CIS Controls Assessment Artifact Request

Agency Name

Date:

1 April, 2025

Purpose

The purpose of this document is to establish a standardized list of artifacts for evaluating the implementation of the Center for Internet Security’s (CIS) Critical Security Controls, in accordance with the CIS Controls Assessment Specification (CIS CAS). Derived directly from the CIS CAS, this list is provided to the assessment point of contact by Assessors prior to an assessment to allow sufficient time for the gathering of required artifacts.

Scope

Agency-owned information and systems, whether on-premises, in the cloud, or administered through a managed service provider. The CIS Safeguards assessed are selected from Implementation Groups 1 and 2 of Version 8 of the CIS Controls.

Applicability

The following requested artifacts are applicable to the CIS Version 8.0 Critical Security Controls, Implementation Group 1 (IG1), and constituent safeguards, as well as a select subset of controls and constituent safeguards from Implementation Group 2 (IG2) and Group 3 (IG3) for which there are Enterprise service offerings.

The artifacts listed below follow the guidance set forth by and applicable to the CIS CAS. The CIS CAS is intended to provide a common understanding of what should be measured to verify that CIS Safeguards are properly implemented.

Artifact Request Guidance

Artifacts may be submitted in any format such as Excel documents, Word documents, Visio Drawings in PDF or PNG format, screenshots, configuration files, Text files, CSV, or PDFs detailing the configuration settings of security systems. Assessors find it very useful when agencies provide some type of narrative along with any artifacts, however this is not required.

It is important to note that if an artifact does not contain all the required information, it should still be summitted, as it will likely still have value to the assessment.

Each artifact request item below includes a section to indicate the artifact was provided or not, a text box to list the files provided to support the request, and a textbox to provide any additional details that would assist Assessors in reviewing the artifacts provided.

When submitting agency policies or procedures, please be sure the artifact contains a review date and authorized signature.

# **Requested Artifacts**

## **GV01: Detailed Hardware Asset Inventory**

* Maintaining an inventory of all hardware devices on the network helps to ensure that only authorized devices are permitted access to the network, and that unauthorized and unmanaged devices are located and denied access or promptly removed from the network. The purpose of the hardware asset inventory is to serve as ***the authoritative, single source of truth as the baseline against which output from active and passive discovery tools can be compared to look for deltas and to be able to efficiently identify devices that are not authorized.*** ***Output from hardware inventory tools alone does not constitute an authoritative hardware inventory. Hardware inventory tools enumerate software that is in the environment. The authorized hardware inventory defines what should be in the environment.***

Additionally, the hardware inventory plays a critical role in configuration management, planning and executing system backup, incident response, and recovery.

The organization’s detailed inventory of all assets with the potential to receive, store, or process data. Data elements that the inventory should include, at a minimum:

* Hardware (MAC) address
* Machine name
* Asset owner
* Department
* Approval to connect to the network
* Date of last review or update to the inventory

The hardware asset inventory should include, at a minimum, the following types of devices:

* Workstations
* Servers
* Laptops
* Mobile devices (tablets, phones)
* Assets used for remote access (VPN)
* Assets used for administrative purposes (e.g. privileged-access workstations)
* Discovery/Vulnerability Scanners (i.e. Tenable.sc)

Artifact provided.  Artifact not provided.

List file names provided for this artifact below:

       
Any Additional Details you wish to provide

## **GV03: Configuration Standards**

Documented configuration standards will be used by assessors to validate implementation of select safeguards. For example, the CIS Controls Assessment Specification for Safeguard 1.3 – Utilize an Active Discovery Tool – requires that assessors review the configuration standard for the organization’s active discovery tool(s) to validate breadth of coverage for the tool(s) as well as to confirm that the tool(s) is / are configured to interface with the organization’s asset inventory to make automatic updates. The CIS CAS for Safeguard 4.9 requires that assessors review the organization's DNS configuration standard to validate that the organization is configuring its systems to leverage trusted DNS servers.

Examples of configuration standard submissions include, but are not limited to: Group Policy objects (GPOs), industry standard configuration baselines (CIS Benchmarks, IRS SCSEMs, DISA STIGs, USGCB, etc.), screen shots from tools that show the appropriate configuration settings, and output from command line tools or utilities.

Documented and approved Configuration Standard (e.g. Agency developed configuration standards, CIS Benchmarks, IRS SCSEMs, DISA STIGs, and USGCB) with a date of last review for the following:

* Operating systems and software
  + Workstations and servers
  + Mobile devices (Phones, Tablets, etc.)
  + Browsers
  + Microsoft 365
* Active discovery tools
  + Active discovery scan policy
  + Scan target list(s)
  + Bash script(s) used to automate discovery scan(s)
  + Nmap syntax used for discovery scan(s)
  + MASSCAN syntax used for discovery scan(s)
  + Timestamp(s) showing scan execution time
  + Any other applicable scan configuration artifacts to validate breadth and depth of scan coverage.
* Encryption software / mechanisms – for end-user devices
  + BitLocker encryption
  + Configuration standard for other encryption software in use
* DNS servers
  + Screen shot of DNS server configured forwarders showing enterprise “CAT” servers.
* Accounts on externally‐exposed applications
* Authorized remote access assets
* Account naming convention for regular, privileged and service accounts
* Administrative accounts
* Automated patch management software / mechanisms
* Vulnerability scanners / scanning software
* Multi-factor authentication (MFA)
  + For administrative accounts (all accounts including DCS, on-premise Active Directory)
  + For remote network access

Agencies must provide documented deviations from any configuration baselines in use at the agency.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV05: Authorized Software Inventory**

The purpose of the authorized software inventory is to serve as the ***authoritative, single source of truth as the baseline against which output from software discovery tools can be compared to look for deltas and to be able to efficiently identify software that is not authorized.*** ***Output from software inventory tools alone does not constitute an authoritative software inventory. Software inventory tools enumerate software that is in the environment. The authorized software inventory defines what should be in the environment.***

Additionally, the software inventory helps to ensure that software running in the organizational environment is supported and receiving vendor updates, and that unnecessary software is not running on organizational devices, exposing the organization to unnecessary risk. The software inventory is also a necessary component for the organization to document and track exceptions for software that is beyond end-of-life and no longer supported but is necessary for the fulfilment of the organization’s mission and business purpose.

Detailed inventory of all licensed, and approved software installed on the organization’s assets. Data elements that the software inventory must document, at a minimum, include:

* Software title
* Software publisher
* Initial use or software approval date
* business purpose
* Software supported / unsupported
* Date of last review & update

Software listed in the inventory should include, but is not limited to:

* Authentication, Authorization, and accounting (AAA) Systems
* Directory and SSO services
* Authorized browsers
* Authorized email clients
* Authorized browser & email plugins
* Authorized operating systems
* Authorized anti‐malware software
* Authorized patch management software
* Authorized backup software
* Authorized host‐based intrusion detection software
* Authorized host‐based intrusion prevention software
* 802.1x authenticators
* Application layer filtering software
* Encryption software

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV10: Organization's Data Management Process**

Documented and approved process that describes how the organization ensures that data is collected, processed, stored, and disposed of in a secure and consistent manner. This may or may not include agency information found in Oregon special records retention schedules.

The data management process must address, at a minimum:

* Data sensitivity
* Data ownership
* Handling of data
* Data retention limits
* Disposal requirements based on data classification

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV12: Sensitive Data Inventory**

Documented and approved list that contains, at a minimum, all sensitive data that the organization generates, collects, or processes in pursuit of its mission and business purposes. This may or may not include agency information found in Oregon special records retention schedules.

The organization’s inventory of sensitive information must include, at a minimum:

* Date of last review and update to the data inventory
* Data classification / sensitivity levels for each data set in the inventory
* Classification / sensitivity levels should be consistent with the organization’s data management process.
* Applicable data retention timeframes, consistent with the organization's data management process
* Data owner(s) for each data set in the inventory.
* For each data set, mapping to assets storing the data (data storage location)

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV18: Enterprise Assets Storing Sensitive Data**

Provide an inventory of any system, applications, or databases within the agency that processes, transmits or stores sensitive data. Sensitive Data at minimum would be data classified at Level 3 or higher

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV20: Unique Password Policy**

The organization’s official policy dictating the minimum password construction and complexity requirements to be employed for password creation and use.

The unique password policy must address, at a minimum:

* Prescriptive requirements for managing default accounts (e.g. disabling, changing default passwords for, etc.)
* Strength of mechanism requirements for accounts (i.e. Password length, minimum and maximum password age, and password history).

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV22: Inventory of Accounts**

The purpose of the inventory of accounts is to serve as the authoritative, ***single source of truth as the baseline against which output from account inventory and management tools (e.g. Active Directory, PowerShell, etc.) can be compared to look for deltas*** and to be able to efficiently identify accounts that are not authorized, accounts that are no longer necessary, and accounts that are no longer in use. ***Account inventory and management tools enumerate accounts that are in the environment. The account inventory defines what should be in the environment.***

Documented inventory of all accounts authorized to access agency systems and components.

The organization’s inventory of accounts must contain, at a minimum, all standard, service, and administrator accounts:

* Account owner’s full name
* Username
* Start date
* Stop date
* Department
* Date of last review and update to the inventory of accounts

Account types should include, but are not limited to:

* Domain accounts
  + standard user
  + administrator
  + service accounts
* Local system user and or admin accounts
* Database accounts
* Internal application accounts
* External application accounts

***Output from account inventory and management tools alone does not constitute an authoritative inventory of accounts.***

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV24: Authorized Automated Patch Management Software**

A list of all automated patch management software that the organization uses to perform application updates on organization software. Will be a subset of GV05 – Authorized Software Inventory and GV03 – Configuration Standards.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV25: List of Vulnerability Scanning Software**

A list of all vulnerability scanning software that the organization uses to perform automated vulnerability scans of internal and external assets. Will be a subset of GV05 – Authorized Software Inventory and GV03 – Configuration Standards.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV26: Agency Audit Log Management Process**

Documented and approved process that defines the enterprise’s logging requirements. The audit log management process must address, at a minimum:

* Instructions for the collection of audit logs
* Instructions for review of audit logs
* Instructions for retention of audit logs
* The date of last review and update to the audit log management process

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV31: List of Authorized Anti‐malware Software**

A list of all anti-malware software that the organization deploys on organization assets. Will be a subset of GV05 – Authorized Software Inventory and GV03 – Configuration Standards.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV43: List of workforce members**

Organization’s list of current workforce members including all staff, volunteers, vendors, partners, etc. Agencies may want to reach out to their local Workday coordinator to assist in obtaining this list. The list should include at a minimum:

* Full Name
* Position
* Start Date
* Employee Classification (Full and Part Time Staff, Contractors, Vendors, Volunteers, etc.)

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV44: Service Provider Inventory List**

Formal, approved list of all external service providers, including vendors, suppliers, contractors, cloud service providers, and other third-party partners that the organization leverages for the maintenance and operation of the information technology that it uses in the fulfilment of its mission and business purpose.

The service provider inventory list should include, at a minimum, the following information:

* Name of service provider
* Security classification of the service provider
* Agency contact for the service provider
* Service Provider contact for the agency
* The date of last review and update to the service provider inventory list

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV51: Agency Incident Response Documentation**

Organization’s approved, documented incident response plan or other incident response documentation that provides direction to organization personnel for incident response and recovery efforts.

Incident response documentation should include, at a minimum, the following information:

* Documents dedicated personnel to manage incident handling:
  + Primary personnel
  + Backup personnel
  + Roles & responsibilities for primary personnel
  + Roles & responsibilities for backup personnel
* Contact information for reporting security incidents
* Process for reporting security incidents
  + Reporting timeframe
  + Personnel to report to
  + Mechanism for reporting
  + Minimum information to be reported in the event of a security incident
* Date of last review & update to the incident response documentation

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **GV54: Most recent external penetration test report for the organization**

Penetration testing is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weaknesses in a system’s defenses which attackers could exploit. Agencies may redact any information they do not wish to share with this assessment.  
Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD01: IP Address Management Documentation for the Organization**

IP address documentation for the organization that includes:

* A comprehensive list of all IP addresses allocated to and managed by the organization
* Details of any associated subnets and ranges
* If applicable, information on whether these IP addresses are actively in use, reserved, or retired
* Any relevant metadata (e.g. devices assignment, location, or purpose.)
* Be sure to include both internal and external address ranges in use by the agency.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD02: Agency policy documentation that defines the timeframe for removing unauthorized devices**

Approved, documented policy that defines the timeframe within which unauthorized devices must be removed from the organization’s network, or otherwise addressed, when discovered.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD03: List of Active Discovery Tool(s) Used by the Organization**

A list of all active discovery tools that the organization uses to identify assets connected to its network. Will be a subset of GV05 – Authorized Software Inventory and GV03 – Configuration Standards.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD04: Exception Documentation for Unsupported Software That is Necessary for the Fulfillment of the Organization's Mission**

Approved exception documentation for software that is unsupported yet necessary for the fulfillment of the organization’s mission and business purpose.

The exception documentation should document the following information:

* Name of the unsupported software
* Software publisher
* Software version
* The business need for the unsupported software
* Initial use or software approval date
* Name of authorizing official
* Exception Approval date
* Exception review date for renewal of exceptions
* Compensating controls
* Acceptance of residual risk
* Date of last review & update

Exception documentation will be compared against unauthorized software discovered in the organization’s environment, to identify instances of unauthorized software for which the organization has formally documented an appropriate exception.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD05: Policy Documentation That Defines the Timeframe Between Consecutive Active Software Discovery Scans**

Approved, documented policy that defines the maximum timeframe allowed between active software discovery scans for the organization.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD06: List of Software Inventory Tools in use by the Organization**

A list of all software inventory tools that the organization uses to automate the discovery and documentation of installed software in its environment. Will be a subset of GV05 – Authorized Software Inventory and GV03 – Configuration Standards.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD07: Process for Granting Access to Organization Assets**

Documented and approved process for granting access to organization assets. The access granting process should include, at a minimum:

* Instructions for granting access upon new hire
* Instructions for granting additional access for existing users or roles
* Instructions for managing access for user role changes

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD08: Process for Revoking Access to Organization Assets**

Documented and approved process for revoking access to organization assets. The access revocation process should include, at a minimum:

* Instructions for revocation of access upon termination of employment
* Instructions for revocation of extraneous access for existing personnel or roles
* Instructions for revocation of access upon role change of a user

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD09: Organization Vulnerability Management Process**

The organization’s documented and approved process for handling vulnerabilities, including, but not limited to vulnerability scanning, and patch management for both OS and third-party software.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD10: Organization Vulnerability Remediation Process**

Organization’s documented risk-based vulnerability remediation process. The risk-based procedure must go beyond vulnerability scores and include environmental factors such as prevalence of vulnerabilities, exposure of systems, sensitivity of systems, impact of exploitation, and ease of exploitation.

The organization’s vulnerability remediation strategy may be documented as part of its vulnerability management process, or in a separate process document.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD11: Documented Data Recovery Process for the Organization**

Organization’s documented and approved process to scope and define critical systems for data recovery. The data recovery process must include, at a minimum:

* Scope of data recovery activities
* Recovery prioritization
* Security of backup data
* Date of last review and update of the data recovery process

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD12: Agency Security Awareness Training Program Plan**

Organization’s documented security awareness training program plan for educating organization personnel on how to interact with organization data and assets in a secure manger. Agencies may leverage the Statewide Information Security Plan if they do not maintain their own Awareness Training plan; however, agencies must document that they have adopted the Statewide Awareness Training Plan.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD13: List of all remote access technologies in use by the organization**

List of all technologies that the organization uses for remote access to organization systems and data. Please also provide a screenshot, or other artifact showing each technology enforcing MFA.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

## **AD14: Security Awareness and Training metrics for the prior year**

Security Awareness and Training metrics for the prior calendar year, showing the total population of organization workers required to complete training, and the total population of workers that have completed the training. Please be sure the report includes Name, Start Date in Position, Enrollment Status, and completion status.

Artifact provided.  Artifact not provided.

List file names for this artifact below:

Any Additional Details you wish to provide

# Applicable Safeguards and Statewide IT Control Standards

* GV01 Applicable Safeguards:  
  1.01, 1.02. 1.03, 2.03 ,2.04, 3.02 ,3.06, 4.01, 4.02, 4.03, 4.04, 4.05, 4.06, 4.07, 4.09, 6.04, 7.03, 7.04, 7.05, 7.06, 8.02, 9.02, 10.01, 10.03, 11.02, 12.01

GV01 Statewide Information Technology (IT) Control Standards:  
CM-8, CM-8(1), PM-5

* GV03 Applicable Safeguards:  
  1.03, 3.06, 4.01, 4.02, 4.03, 4.04, 4.05, 4.06, 4.09, 6.03, 6.05, 7.03, 7.04, 7.05, 7.06, 9.02, 10.01, 10.02, 10.03, 11.02, 11.03, 11.04

GV03 Statewide Information Technology (IT) Control Standards:  
CM-1, CM-2, CM-6, CM-7, CM-7(1), CM-9, SA-3, SA-8, SA-10

* GV05 Applicable Safeguards:  
  2.01, 2.02, 2.03, 3.06, 4.01, 4.02, 4.03, 4.04, 4.05, 4.06, 4.07, 5.01, 6.03, 7.03, 7.04, 7.05, 9.01, 9.02, 10.01, 11.02

GV05 Statewide Information Technology (IT) Control Standards:  
CM-7(1), CM-8, MA-3

* GV10 Applicable Safeguards:  
  3.01

GV10 Statewide Information Technology (IT) Control Standards:  
AU-11, CM-12, SI-12, MP-6, SR-12

* GV12 Applicable Safeguards:  
  3.02, 3.04, 3.05, 3.07

GV12 Statewide Information Technology (IT) Control Standards:  
CM-12, PM-5(1), RA-2, AU-11, SI-12, MP-6, SR-12, RA-2

* GV18 Applicable Safeguards:  
  7.02, 8.05

GV18 Statewide Information Technology (IT) Control Standards:  
IA-5(1), SC-28, SC-28(1), RA-5,

* GV20 Applicable Safeguards:  
  4.07, 5.02

Statewide Information Technology (IT) Control Standards:  
IA-2(1), IA-2(2) , IA-5, IA-5(1)

* GV22 Applicable Safeguards:  
  5.01, 5.03, 5.04, 6.03, 6.05

GV22 Statewide Information Technology (IT) Control Standards:  
AC-2, AC-2(3), AC-6(2), AC-6(5), IA-2(1), IA-2(2)

* GV24 Applicable Safeguards:  
  7.04

GV24 Statewide Information Technology (IT) Control Standards:  
RA-5, RA-7, SI-2, SI-2(2)

* GV25 Applicable Safeguards:  
  7.05, 7.06

GV25 Statewide Information Technology (IT) Control Standards:  
RA-5

* GV26 Applicable Safeguards:  
  8.01. 8.02, 8.03

GV26 Statewide Information Technology (IT) Control Standards:  
AU-1, AU-2, AU-4, AU-7, AU-12

* GV31 Applicable Safeguards:  
  7.04

GV31 Statewide Information Technology (IT) Control Standards:  
RA-5, RA-7, SI-2, SI-2(2)

* GV43 Applicable Safeguards:  
  14.01, 14.02, 14.03, 14.04, 14.05, 14.06, 14.07, 14.08

GV43 Statewide Information Technology (IT) Control Standards:  
AT-1, AT-2, PM-13

* GV44 Applicable Safeguards:  
  15.01

GV44 Statewide Information Technology (IT) Control Standards:  
PM – 30(1)

* GV51 Applicable Safeguards:  
  17.01, 17.02, 17.03

GV51 Statewide Information Technology (IT) Control Standards:  
IR-1, v IR-5, IR-6, IR-6(1), IR-6(3), IR-7, IR-8

* GV54 Applicable Safeguards:  
  18.01, 18.02

GV54 Statewide Information Technology (IT) Control Standards:  
None

* AD01 Applicable Safeguards:  
  01.01

AD01 Statewide Information Technology (IT) Control Standards:  
CM-8

* AD02 Applicable Safeguards:  
  1.02

Statewide Information Technology (IT) Control Standards:  
CM-8(3)

* AD03 Applicable Safeguards:  
  1.03

AD03 Statewide Information Technology (IT) Control Standards:  
SI-4

* AD04 Applicable Safeguards:  
  2.02

AD04 Statewide Information Technology (IT) Control Standards:  
SA-22

* AD05 Applicable Safeguards:  
  1.03

AD05 Statewide Information Technology (IT) Control Standards:  
SI-4

* AD06 Applicable Safeguards:  
  2.04

AD06 Statewide Information Technology (IT) Control Standards:  
SI-4

* AD07 Applicable Safeguards:  
  6.01

AD07 Statewide Information Technology (IT) Control Standards:  
IA-4, IA-5, AC-1, AC-2, AC-2(1)

* AD08 Applicable Safeguards:  
  6.02

AD08 Statewide Information Technology (IT) Control Standards:  
AC-1, AC-2, AC-2(1)

* AD09 Applicable Safeguards:  
  7.01

AD09 Statewide Information Technology (IT) Control Standards:  
RA-5

* AD10 Applicable Safeguards:  
  7.02

AD10 Statewide Information Technology (IT) Control Standards:  
RA-5

* AD11 Applicable Safeguards:  
  11.01

AD11 Statewide Information Technology (IT) Control Standards:  
CP-2, CP-10

* AD12 Applicable Safeguards:  
  14.01, 14.02, 14.03, 14.04, 14.05, 14.06, 14.07, 14.08

AD12 Statewide Information Technology (IT) Control Standards:  
AT-1, AT-2, PM-13

* AD13 Applicable Safeguards:  
  6.4, 6.5

AD13 Statewide Information Technology (IT) Control Standards:  
AC-19, IA-2(1), IA-2(2)

* AD14 Applicable Safeguards:  
  AT-1, AT-2, AT-2(3), PM-13, AC22

AD14 Statewide Information Technology (IT) Control Standards:  
N/A