

State of Ohio IT Standard

Standard Number: ITS-SEC-02	Title: Enterprise Security Controls Framework
Effective Date: 4/18/2011	Issued By: Stuart R. Davis, Assistant Director/State CIO Office of Information Technology Department of Administrative Services
Version Identifier: 1.0	Published By: Office of Information Security & Privacy

1.0 Purpose

This state IT standard specifies the minimum requirements for information security in all **agencies** and identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53, revision 3 (NIST 800-53) as the framework for information security controls implementation for the state.

2.0 Scope

Pursuant to Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," this state IT standard is applicable to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government except for those specifically exempted. Non-participating agencies are encouraged to comply with this standard as well as all enterprise policies, standards and guidelines.

3.0 Background

Ohio established the Chief Information Security Officer (CISO) Leadership Subcommittee under the auspices of the Multi-Agency CIO Advisory Council (MAC) in 2010. One of their first tasks was to evaluate available options for establishing an information security controls framework for the state. They chose NIST 800-53 to be that framework. After review by the MAC, adoption of this framework was recommended to the State Chief Information Officer.

Adoption of this common framework of information security controls for the state offers several advantages.

- Agencies can share a common vocabulary and common set of concepts related to information security controls, which will improve communication and understanding of this topic within and among the agencies.

- Agencies will be able to share expertise, documentation, training materials, and processes, which will allow for more cross-agency collaboration.
- A common standard can be established for auditing and common methods established for compliance monitoring.
- When everyone is using the same information security controls framework, greater insight into the overall security posture of the state can be available, which can help determine the most efficient and effective deployment of security resources.
- Using NIST 800-53 as its security controls framework allows the state to leverage research already performed and implementation guidance already produced by the federal government and provides the opportunity for better alignment between state and federal security requirements.

The complexity involved in securing agency systems can be enormous and focus is necessary to ensure that limited resources are prioritized and applied to the areas of the highest risk. Significant work has been done to address this concept and the result is the Consensus Audit Guidelines or CAG, published by the SANS Institute. The CAG is a subset of security controls in NIST 800-53. The controls identified in the CAG address the highest threat areas for the enterprise environment. The CAG has emerged as a prioritized baseline or high water mark “to address the attacks occurring today as well as those anticipated in the near future.” It is recommended by the authors of CAG that these controls be “assessed as the baseline set of ‘Common Controls’...as defined by NIST.”

Given the effort involved with implementing NIST 800-53, Ohio felt it was critical to ensure that high risk, high priority IT security threats were addressed immediately. Therefore, the State CIO, CISO and the CISO Leadership Committee identified a set of **enterprise controls**.

In the interest of securing against the most imminent and likely threats, Ohio is requiring that agencies make the implementation of the enterprise controls a top priority. (Refer to Section 8.0 for more detail regarding implementation expectations.)

4.0 Standard

State agencies shall use the NIST 800-53, as the basis for selecting information security controls. The selection of individual controls must be based upon **system classification** and an overall understanding of risks posed to that system.

The implementation of the controls within the NIST framework will vary to some degree across the enterprise based upon system classification and risks posed to those systems.

In order to establish an information security baseline across all state agencies and address the currently known high-priority attacks agencies are required to implement the enterprise controls listed below.

4.1 Enterprise Controls

4.1.1 Program Management

All agencies must develop an information security program consistent with the requirements outlined in the PM family of controls in NIST 800-53.

4.1.2 Inventory of Authorized and Unauthorized Devices

Agencies must implement a method to create and maintain an inventory of authorized and unauthorized devices connected to the agency's network consistent with guidance in the CAG.

4.1.3 Inventory of Authorized and Unauthorized Software

Agencies must implement a method to create and maintain an inventory of authorized and unauthorized software deployed throughout the agency consistent with guidance in the CAG.

4.1.4 Secure Configurations for Hardware and Software on Laptops, Workstations and Servers

Agencies must adopt common configurations with documented security configurations consistent with guidance in the CAG.

4.1.5 Secure Configurations for Network Devices such as Firewalls, Routers and Switches

Agencies must adopt and document standard secure configurations for all network devices deployed within the agency consistent with guidance in the CAG.

4.1.6 Boundary Defense

Agencies must implement boundary defenses consistent with the guidance in the CAG.

4.1.7 Maintenance, Monitoring and Analysis of Security Audit Logs

Agencies must implement auditing and logging capabilities consistent with guidance in the CAG and the AU family of controls within NIST 800-53.

4.1.8 Application Software Security

Agencies must implement application security controls consistent with the guidance in the CAG.

4.1.9 Controlled Use of Administrative Privileges

Agencies must implement controls around administrative privileges consistent with the guidance in the CAG.

4.1.10 Controlled Access Based on Need-to-Know and Least Privilege

Agencies must implement access controls based upon the principles of need-to-know and least privilege consistent with guidance in the CAG and the AC family of controls in NIST 800-53.

4.1.11 Continuous Vulnerability Assessment and Remediation

Agencies must develop continuous vulnerability assessment and remediation capabilities, policies and procedures consistent with guidance in the CAG and in the RA family of controls in NIST 800-53.

4.1.12 Account Monitoring and Control

Agencies must implement controls to monitor and control system and user accounts consistent with the guidance in the CAG.

4.1.13 Malware Defenses

Agencies must implement anti-malware technologies and configure them consistent with the guidance in the CAG. For the purposes of this control mobile devices do not include smartphones however; agencies are strongly encouraged to evaluate the need for anti malware technologies for smartphones and other handheld devices to the extent that they are in use within the agency.

4.1.14 Limitation and Control of Network Ports, Protocols and Services

Agencies must implement controls to limit the use of network ports and services to only those that have a business purpose. Further, agencies should periodically review existing ports and services to ensure that the need remains.

4.1.15 Wireless Device Control

Agencies must implement controls to protect wireless devices which are consistent with the guidance in the CAG.

4.1.16 Data Loss Prevention

Agencies must evaluate the need for data loss prevention technologies within their environments. Agencies that handle, store or process sensitive, confidential or other information that is required to be protected by law, regulation or Executive Order must implement data loss prevention technologies consistent with the guidance in the CAG.

4.1.17 Secure Network Engineering

Agencies must follow secure network engineering/architecture standards which are consistent with guidance in the CAG.

4.1.18 Penetration Tests and Red Team Exercises

Agencies must perform penetration testing on a periodic basis to ensure the effectiveness of the implemented controls. Additionally, agencies should consider having external teams perform exercises to further assess the efficacy of their defenses consistent with guidance in the CAG.

4.1.19 Incident Response Capability

Agencies must establish incident response capabilities consistent with the guidance in the CAG including but not limited to developing policies and procedures for how incidents will be handled. Because of the sensitive nature of incident response and investigation, agencies should involve their Chief Legal Counsel as well as Human Resources in this

development. Additionally, agencies should test their incident response procedures periodically to ensure they remain viable.

4.1.20 Data Recovery Capability

Agencies must develop and implement data recovery capabilities consistent with guidance in the CAG.

4.1.21 Security Skills Assessment and Appropriate Training to Fill Gaps

Agencies must develop and implement security education and training capabilities consistent with guidance in the CAG and in the AT family of controls in NIST 800-53.

4.2 Revisions to this Standard

The Office of Information Security and Privacy shall ensure that this standard is regularly reviewed and updated as needed. The current version of NIST 800-53 is Revision 3 (August 2009). Future revisions to NIST 800-53 will be considered for inclusion after final publication.

4.3 Exceptions to this Standard

In general, there are no exceptions to this state IT standard. However, agencies do have the latitude to make risk-based decisions on controls listed within the NIST 800-53 baselines. The decision not to implement a specific control or control enhancement must be documented and approved by agency leadership.

5.0 References

- 5.1** Ohio IT Policy ITP-A.1, *Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services*, defines the authority of the state CIO to establish State of Ohio IT standards as they relate to the acquisition and use of information technology by state agencies, including, but not limited to, hardware, software, technology services and security.
- 5.2** NIST Special Publication 800-53 (Rev 3), *Recommended Security Controls for Federal Information Systems and Organizations*, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.
- 5.3** *Twenty Critical controls for Effective Cyber Defense: Consensus Audit Guidelines*, defines the consensus of security professionals, law enforcement, and CIOs for both the public and private sectors on baseline security controls that have been effective in blocking currently known high-priority attacks. This document provides a “first step towards providing specific guidelines that CISOs, CIOs, IGs and various Computer Emergency Response Teams can adopt...to ensure that their systems have the most critical baseline security controls in place.”
- 5.4** Cyber Security Evaluation Tool (CSET), is an IT security assessment tool developed by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD). This desktop software tool guides users through a step-by-step process to collect facility-specific control system information that addresses topics such as hardware, software, administrative policies, and user obligations. It then compares that information to relevant security standards and regulations, assesses overall compliance, and provides appropriate

recommendations for improving the system's cyber security posture. (Copies of this software have been provided by DHS and are available from the Office of Information Security and Privacy.)

6.0 Definitions

Agency or Agencies

Every organized body, office, or agency established by the laws of the state for the exercise of any function of state government, other than any state-supported institution of higher education, the office of the auditor of state, treasurer of state, secretary of state, or attorney general, the adjutant general's department, the bureau of workers' compensation, the industrial commission, the public employees retirement system, the Ohio police and fire pension fund, the state teachers retirement system, the school employees retirement system, the state highway patrol retirement system, the general assembly or any legislative agency, or the courts or any judicial agency.

Enterprise Controls

IT security controls that were selected by the State CIO, CISO, and the CISO Leadership Committee. The controls are a representation of all of the top 20 CAG controls and select NIST Special Publication 800-53 controls. While the long-term goal for agencies is the implementation of the full NIST Special Publication 800-53 framework, implementation of the selected enterprise controls should be the short-term, immediate focus for agencies.

System Classification

Refers to the process of assessing the potential impact to confidentiality, integrity and availability of the evaluated system. In the NIST 800-53 publication they refer to FIPS-199 which is the Federal guidelines for assessing and classifying information systems. The Office of Information Security and Privacy will be developing further guidance around system classification but agencies can utilize the FIPS-199 publication until further guidance is released.

7.0 Related Resources

Document Name
FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems is available at the following location: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
NIST Special Publication 800-53 Revision 3 and other NIST Special Publications of interest to the information security community can be found at the following location: http://csrc.nist.gov/publications/PubsSPs.html
The <i>"Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines"</i> is available from the SANS Institute at the following location: http://www.sans.org/critical-security-controls/guidelines.php
Copies of related resources will also be available on the Ohio Privacy & Security Information Center: http://www.infosec.ohio.gov

8.0 Implementation

Implementing or retrofitting an information security architecture is not something that is done overnight. Other states have adopted the NIST framework and have taken several years to reach full implementation. For this reason Ohio has adopted the following implementation roadmap as a starting point and guide for agencies to follow in implementing this architecture within their respective environments.

The first step in the process should be to perform a gap analysis to determine alignment of current controls with the NIST framework. One way to accomplish this is by utilizing the CSET tool provided by the US Department of Homeland Security. The results of this evaluation should provide a starting point for prioritizing. It is highly suggested that agencies utilize the enterprise assessment as opposed to the NIST Special Publication 800-53 assessment to start. The NIST Special Publication 800-53 assessment is a system based assessment and best utilized to evaluate compliance in a single system.

- 8.1** Agencies are expected to work towards implementation of the NIST framework as quickly as feasible.
- 8.1.1 In new systems, the control baselines in NIST 800-53 shall immediately become requirements for the system.
 - 8.1.2 For existing systems and systems that have moved beyond the requirements phase, control decisions must be made and documented based upon a gap analysis between the appropriate NIST 800-53 baseline and the existing controls within the system.
 - 8.1.3 Agencies shall utilize the information security program plan and the plan of action and milestones process required in the NIST 800-53 PM family of controls to document progress made in implementing this standard as well as documenting how the agency will address any gaps.
 - 8.1.3.1 The Information Security and Privacy Office will release additional guidance about the format and required information to be included in the information security program plan. The combination of the information security program plan and the plan of actions and milestones will serve as the strategic plan required in ORC 125.18 (C) (1).
 - 8.1.4 Agencies shall also consider guidance within NIST 800-53 Section 3.3 in working with external providers to ensure that externally hosted systems are protected to an acceptable level.
- 8.2** The implementation of the enterprise controls listed within section 4.1 of this standard is expected within 18 months of the effective date of this standard.
- 8.3** Agencies are encouraged to evaluate the need for hiring a security professional to assist them in building their information security program. The Office of Information Security and Privacy is also available to assist agencies in selecting and implementing security controls.

9.0 Revision History

Revision Date	Description of Changes
04/18/2011	Version 1.0, original standard

10.0 Inquiries

For information regarding this state IT standard or the NIST Special Publication 800-53 security controls framework, please contact:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, Suite 4083
Columbus, Ohio 43215
Telephone: 614.644.9391
Email: state.isp@oit.ohio.gov
Web: infosec.ohio.gov

State of Ohio IT Standards can be found online at: www.ohio.gov/itp

11.0 Attachments

None.