Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Standard

Office Instruction:	**CSO-STD-2005**
Office Instruction Title:	**System Monitoring Standard**
Revision Number:	**2.0**
Effective Date:	**September 30, 2019**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Description:	CSO-STD-2005, “System Monitoring Standard,” provides the minimum security requirements that must be met for system monitoring.
Training:	As request

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	6/25/19
CISO	Jonathan Feibus	/RA/	6/28/19

TABLE OF CONTENTS

Computer Security Standard
CSO-STD-2005

System Monitoring Standard

---

1 PURPOSE

CSO-STD-2005, "System Monitoring Standard," provides the minimum security requirements that must be applied to all systems operated by, or on behalf of, the Nuclear Regulatory Commission (NRC) processing or storing information including unclassified, Safeguards Information (SGI), and the classified level.

This standard is intended to be used by system owners, system administrators, system and solution architects, information technology (IT) system managers (operational and project-related), and Information System Security Officers (ISSOs) to ensure that system monitoring is performed.

This standard does ***not*** apply to incident handling.

2 GENERAL REQUIREMENTS

NRC systems are required to be monitored to assist in detecting, responding to, and following up after potential cybersecurity events/incidents. This section provides the high-level requirements addressing system monitoring procedures, audit log information maintained to assist with monitoring, how potential conflicts with classified requirements from other sources are addressed, and how potential conflicts with applicable security configuration baselines are handled.

All system components (e.g., servers) on the NRC production network should be configured to send their system logs to the agency's centralized logging solution, where applicable.

Capturing and monitoring system event information assists the agency with detecting and responding to misuse, and maintaining system integrity.

All NRC system monitoring must comply with all federally mandated and NRC-defined security requirements.

This standard provides requirements that must be used in concert with:

- Computer Security Incident Response Team (CSIRT) Process
- CSO-STD-0020, "Organization-Defined Values for System Security and Privacy Controls"

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, (as amended), "Security and Privacy Controls for Federal Information Systems and Organizations"

2.1 System Monitoring Procedures

NRC systems must have system monitoring procedures documented and maintained that define and specify how the following steps are performed:

1. Gather, report, and produce alerts based upon computer system monitoring (e.g., audit/logging) information;
2. Assign the system ISSO and other security operations individual(s)/group(s), as appropriate, to review system monitoring information on a periodic basis, per CSO-STD-0020, upon receipt of alerts, notification of potential security events/incidents, and any other cases where appropriate;
3. Identify what appears to be suspicious or potentially suspicious successful or failed activity for the system;
4. Document the results of the review of system monitoring information as per ISSO's discretion and share with individuals with cybersecurity responsibilities (e.g., system ISSOs, office ISSOs, IT system managers, Computer Security Organization [CSO] points of contact for office); and
5. Report suspicious or potentially suspicious activity to CSIRT and execute incident response activities, as appropriate.

Systems must provide the capacity to produce activity reports that facilitate the review of system audit log information, including automatic processing to identify events of interest (e.g., query capabilities).

Automated tools (e.g., Splunk, Panorama) may be utilized to ingest, correlate, produce alerts, and assist with the completion of system monitoring reviews. These tools can provide significant value in automatically evaluating and identifying trends, highlighting events of interest, and producing alerts/notifications of potential security incidents or suspicious events.

2.2 Maintain Audit Logs

Audit log information (e.g., events audited, attributes captured) must be maintained to permit NRC to:

- Detect attacks, indicators of potential and actual attacks, or identify suspicious activity within the information system and across boundaries of the system (e.g., boundaries with NRC systems and other areas, such as the internet);
- Respond to and contain attacks; and
- Support after action analysis and forensic investigations in the event of potential or actual breaches.

2.3 Resolve Potential Conflicting Requirements with Classified Systems

Classified systems must follow all applicable system monitoring, auditing, and logging requirements specified by the Committee for National Security Systems (CNSS) and the National Security Agency (NSA). If there are any conflicts between the requirements stated in this standard and CNSS or NSA requirements, the CNSS or NSA requirements shall take precedence over the requirements in this standard.

2.4 Resolve Potential Conflicting Requirements with Applicable Security Configuration Baselines

Specific products and technologies within NRC systems must be configured in accordance with applicable security configuration baselines (e.g., external standards) as specified within CSO-PROS-3000, "Cybersecurity Standards Process." These applicable security configuration baselines may include Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) or Center for Internet Security (CIS) Benchmarks. The baselines may specify those type of events that at a minimum are required to be audited, audit attributes that must be captured, audit review frequencies, and other system monitoring related requirements.

Conflicts between security configuration baseline system monitoring settings and requirements found in this standard shall be resolved in the following manner:

- If the security configuration baseline (for a specific product/technology) provides requirements that conflict with or are in addition to those specified in this standard, then the security configuration baseline settings must be followed. The security configuration baseline shall take precedence over this standard.
- However, if the security configuration baseline does not provide system monitoring requirements to be configured, then the requirements in this standard must be followed.

3 SPECIFIC REQUIREMENTS

This section provides the minimum required events to audit, attributes to capture for audited events, and requirements for system monitoring information captured.

3.1 Required Events to Audit

Systems with an overall Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," sensitivity of **Low** or **Moderate** must audit the following events, at a minimum:

- User specific events:
  - User logons, both successful and failed
  - User logoff or session termination
  - Addition, modification, or deletion of data through direct data access by privileged users
  - Changes to account/user, group, or role security privileges/profiles

  - Creation and deletion of accounts/users, roles, or groups
  - All user actions performed by application and backup local administrator accounts
  - Execution of administrative applications and use of administrative interfaces
  - Unsuccessful attempts to access objects (resources) or perform functions that are denied by lack of user privileges or rights
- User or system specific events:
  - Successful accesses to security-critical objects (e.g., operating system, application, and/or server-oriented files, sensitive data)
  - Successful changes to the security configurations, settings, and controls (e.g., operating system, application)
  - Attempts at enabling or disabling of security protection systems (i.e., endpoint protection, anti-virus, anti-malware, firewall, or intrusion detection/prevention systems)
  - Attempts at enabling or disabling auditing
  - Modification of system time or time server configuration
  - Modification or deletion of log files
  - Modification of software or firmware
  - Attempts to elevate rights
  - Attempts to install software
  - Inconsistent pattern of activity
  - System-defined or application-specific events, at the discretion of ISSO (e.g., documented in control implementation summaries of applicable controls within the Audit and Accountability (AU) family of the System Security Plan [SSP])
  - All access to the information system conducted via Out-of-Band (OOB)/lights out management solutions (e.g., Intelligent Platform Management Interface (IPMI), Integrated Dell Remote Access Controller (iDRAC), Hewlett Packard (HP) Integrated Lights Out (iLO), and similar solutions)
  - All access to and actions performed via system orchestration or automated application delivery (e.g., DevOps) tools

In addition to the events above, systems with an overall FIPS 199 sensitivity of **High** and **classified systems** must audit the following additional events, at a minimum:

- Attempts to access, modify, or delete security objects
- Failed attempts to access administrative applications or administrative interfaces;
- Changes to the security configurations, settings, and controls (e.g., operating system, application), both unsuccessful and successful
- Change of sensitive or classified data access rights

- Modification of accounts/users, roles, or groups
- Privileged activities or another system-level access
- Starting and ending time for user access (e.g., remote and local access) to the system
- All concurrent logons (e.g., from different workstations)
- All program initiations
- All direct access to the information system at the local level (e.g., at the system console)

3.2 Required Attributes for Audited Events

Systems must be configured to capture the following attributes, at a minimum, for all events that are audited:

- Date (including month, day, and year) and time of the event (including hour and minute, and must include the specific second, if possible)
- Identity of any individuals or subjects associated with the event (e.g., it must be possible to identify the specific individual performing an action in events performed by a user/account that may be accessed by multiple individuals [e.g., application and backup local administrator accounts])
- Description/type of event
- Source and destination of the event (Internet Protocol [IP] address and hostname)
- Name of the target resource for the event (e.g., application name, system name, record/document name, or file names involved)
- Any change to the system configuration (i.e., settings and new configured values)
- Any change to privileges (e.g., affected account/user/role/group, privilege, and changes made)
- Outcome (success or failure indications)

3.3 Protection of System Monitoring Information

Access to system monitoring information and the ability to enable/disable or reconfigure system monitoring must be assigned under the purview of the system ISSO. This must be done based on the principles of least privilege and separation of duties. The methods used to comply with this requirement must be specified in the control implementation summaries of applicable controls within the AU family of the SSP.

Appendix A. ACRONYMS

AU	Audit and Accountability
CIS	Center for Internet Security
CNSS	Committee on National Security Systems
CSIRT	Computer Security Incident Response Team
CSO	Computer Security Organization
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standard
HP	Hewlett Packard
iDRAC	Integrated Dell Remote Access Controller
iLO	Integrated Lights Out
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Science and Technology
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
OOB	Out-of-Band
SGI	Safeguards Information
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide

Appendix B. GLOSSARY

Forensic Investigation	This is the gathering and analysis of all system or network breach-related evidence to conclude about a suspect.
HP Integrated Lights-Out	This is an embedded server management technology by HP which provides OOB management facilities.
Integrated Dell Remote Access Controller	This is designed as an OOB management platform which allows administrators to improve the availability of Dell servers.
Intelligent Platform Management Interface	This is a set of computer interface specifications for a computer subsystem that provides management and monitoring capabilities independent of the host system's firmware and operating system.
Out-of-Band Management	The exchange of call control information in a separate band from the data or voice stream, or on an entirely separate, dedicated channel. In this case, control information for management network is separate from the rest of network traffic.
Processing Information	Operation or set of operations performed upon information that can include, but is not limited to, collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal or information.

CSO-STD-2005 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
04-Feb-10	1.0	Initial issuance	Distribution at ISSO forum and posting on CSO web page	Upon request
28-Jun-19	2.0	Updated with latest requirements.	Post to OCIO/CSO web page.	Upon request