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

Office Instruction:	**CSO-STD-2108**
Office Instruction Title:	**Endpoint Protection Enterprise Security Architecture Standard**
Version Number:	**2.0**
Effective Date:	**March 31, 2022**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-STD-2108, “Endpoint Protection Enterprise Security Architecture Standard,” provides the minimum security requirements that must be met for the endpoints protection on NRC systems that store or process information up to, and including, the Safeguards Information (SGI) level.
Training:	As requested

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	2/15/22
CISO	Jonathan Feibus	/RA/	2/15/22

TABLE OF CONTENTS

Computer Security Standard
CSO-STD-2108

Endpoint Protection Enterprise Security Architecture Standard

---

1 PURPOSE

CSO-STD-2108, “Endpoint Protection Enterprise Security Architecture Standard,” provides the minimum security requirements for endpoint protection on Nuclear Regulatory Commission (NRC) systems that store or process information up to, and including, the Safeguards Information (SGI) level.

This standard is intended for system administrators, system and solution architects, information technology (IT) system managers (operational and project-related), system owners, and Information System Security Officers (ISSOs) who must ensure application and enforcement of the endpoint protection security requirements.

CSO-STD-2108 is an Enterprise Security Architecture (ESA) standard. ESA standards are not written to define requirements in accordance with the current state of technology in industry or technology that is in use at the NRC. ESA standards are written to provide objective, product-agnostic requirements that are flexible and will remain current for several years following their issuance despite changes in technology. ESA standards provide requirements that are flexible to accommodate both the current and future states of security technologies and products while providing the agency discretion on the selection, use, and configuration of security products.

Refer to CSO-GUID-2108, “Endpoint Protection Enterprise Security Architecture Guidance,” which facilitates compliance with this standard.

This standard does **not** address endpoint protection security requirements for:

- Systems processing classified information.
- Bring Your Own Devices (BYODs) or mobile devices.
  Note: BYOD or mobile endpoint protection requirements will be covered in a future CSO standard.

2 GENERAL REQUIREMENTS

This section addresses the general requirements that all system administrators, system and network architects, and ISSOs authorized to select, administer, and configure endpoint protection within NRC systems must comply with as the minimum set of controls.

All endpoints that are owned or leased and managed and/or operated by the NRC or by parties on behalf of the NRC, must comply with all federally mandated and NRC-defined security requirements.

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

- CSO-STD-4000, “Network Infrastructure Enterprise Security Architecture Standard.”
- CSO-STD-1004, “Laptop Enterprise Security Architecture Standard.”
- CSO-STD-2009, “Cryptographic Control Enterprise Security Architecture Standard.”
- CSO-STD-2005, “System Monitoring Standard.”
- CSO-STD-2008, “Network Ports, Protocols, and Services Enterprise Security Architecture Standard.”

2.1 NRC-Approved Endpoint Protection Products

The NRC Technical Reference Model (TRM) lists hardware and software products that are approved for various purposes, which may include wide or restricted uses. The following requirement applies:

- All products used for endpoint protection must be listed in the NRC TRM as authorized for the identified purpose.

2.2 System Security Plan

This standard provides ISSOs with significant discretion in determining possible products and solutions that can be used to address the full scope of endpoint protection security requirements, as stated in this standard. The following requirement applies:

- ISSOs must document selected endpoint protection solutions and implementations in the System Security Plan (SSP).

2.3 Unauthorized Devices

Unauthorized peripheral devices (e.g., removable media devices) pose a risk to NRC endpoints. Examples of such risk includes, but not restricted to, the potential for data exfiltration or a possible attack with malware. The following requirements apply:

- NRC users are prohibited from connecting unauthorized peripheral devices to NRC endpoints.
- Endpoint protection solutions that are capable of blocking/preventing the use of unauthorized peripheral devices (e.g., prevent use of unauthorized storage peripherals) must technically enforce that prohibition.

3 SPECIFIC REQUIREMENTS

This section identifies specific requirements applicable to NRC user device endpoints (e.g., NRC mobile desktops, NRC loaner mobile desktops) and server endpoints (e.g., physical or virtual servers, gateways, cloud-based platform as a service device) that are a part of the NRC network and systems.

3.1 User Device and Server Endpoints

NRC systems utilize user device endpoints that are used by the NRC employees and contractors to access NRC network resources. Additionally, server endpoints are used, as a part of an NRC network or in a standalone mode, to facilitate such access. The requirements in the following subsections apply to all endpoints.

3.1.1 Antimalware Defense

An antimalware defense solution must be employed on all endpoints that:

- Detect, block, and quarantine malicious code, including viruses, worms, Trojan horses, rootkits, keyloggers, spyware, and adware;
- Detect network-based attacks;
- Allow for creation of an allowlist and blocklist of specific executable binary and script files that are permitted or prohibited from executing; and
- Notify selected individuals upon detection of malicious code.

Supplemental Information: The use of multiple endpoint technologies (e.g., Microsoft Defender, or other Endpoint Detection and Response [EDR] and Extended Detection and Response [XDR] Solutions) to meet this requirement increases the breadth of protection and reduces exposure, such as:

- Antimalware protection solutions protect data by detecting, blocking, and quarantining malicious code using signature-based, and heuristic-based detection mechanisms.
- System application allowlisting and blocklisting provides an additional layer of protection by creating an allowlist and blocklist of specific executables on endpoints beyond the antimalware solution signature files.
- Host-based Application Boundary Protection (ABP) provides an additional layer of security that monitors network-based attacks by analyzing program behavior.

3.1.2 Host-Based Boundary Protection

Host-based boundary protection solutions must be employed on all endpoints. The host-based boundary protection solutions must be configured to:

- Inspect network traffic in real-time during ingress and egress;
- Block prohibited ports, protocols, and services;

- Block network-based attacks; and
- Analyze and block harmful program behavior.

Supplemental Information: The use of both host-based Network Boundary Protection (NBP) and host-based ABP solutions increases the breadth of protection and reduces exposure, such as:

- Host-based NBP can be configured to block network ports, protocols, and services.
- Host-based ABP's heuristic traffic and malware analysis can block network-based attacks for which signatures have not yet been developed.

3.1.3 Monitor for Unauthorized Changes

Endpoint protection solutions must be employed to:

- Monitor changes to executables, services, libraries, drivers, and configuration files for system software and other software on endpoints; and
- Notify selected individuals in real-time upon detection of unauthorized changes to endpoint files.

3.1.4 Malicious and Inappropriate Content Filtering

Endpoint protection solutions must be employed that:

- Block access to known malicious sites; and
- Block access to sites with inappropriate content (e.g., adult sites, gambling sites, file sharing sites).

Supplemental Information: A web content filtering solution blocks access to known malicious sites and sites with inappropriate content. In addition to filtering the content of web pages, the solution mitigates additional potential threats by blocking malware, botnets, keyloggers, and other web threats.

3.1.5 Allow or Block Execution of Applications

Endpoint protection solutions must be configured to allow or block execution of applications or unauthorized software based on:

- A "deny-all, allow-by-exception" policy for all user device endpoints and server endpoints with security categorizations of High; or
- An "allow-all, deny-by-exception" policy for server endpoint with security categorizations of Moderate.

Supplemental Information: A "deny-all, allow-by-exception" approach effectively creates a blocklist even if it is not directly configurable by the system administrator.

3.1.6 Signature-Based Detection and Updates

All endpoint protection solutions that provide signature-based detection capabilities must be configured to automatically update signature files on all endpoints, to ensure that endpoints are protected against the newest threats.

Servers on standalone office local area networks (LANs), such as regional office LANs, that do not have internet access or connectivity to NRC networks to facilitate automatic updates must have signature files updated on a *weekly* basis.

3.1.7 Heuristic Analysis

All endpoint protection solutions that provide heuristic analysis-based detection capabilities must be configured on all endpoints to enable heuristic analysis (i.e., behavioral analysis).

Supplemental Information: The use of antimalware protection and host-based ABP heuristic-based detection to meet this requirement increases the breadth of protection and reduces exposure. The technologies, such as EDR or XDR, provide antimalware protection that has more comprehensive malware heuristic detection than host-based ABP, while host-based ABP has more comprehensive heuristic detection of network-based attacks.

3.1.8 Real-Time Scanning and Notification

All endpoint protection solutions that provide real-time scanning capabilities must be configured to provide real-time scanning of threats, unauthorized changes in software (e.g., system software, malware defense software) and notify selected individuals upon detection of attacks or changes in software. Additionally, the ability to run scans both at scheduled intervals and manually must be utilized for the protection of server endpoints, as appropriate.

Supplemental Information: File integrity monitoring (FIM) is an effective solution to monitor and provide alerts on specific file changes in a system. FIM solutions scan the files on the system to create a baseline of known, good files. The subsequent scans, either in real-time or scheduled, are used to compare the current configuration with the original. Any changes detected are logged and included in reports.

3.1.9 Malicious Code Detection

Malicious code protection solutions must be configured to quarantine infected files and terminate and delete malicious processes upon failure to perform other protective actions.

Supplemental Information: EDR or XDR solutions can be configured to take several actions, in sequence, upon detection of malicious code or suspicious activity, including cleaning, quarantining, or deleting the infected file. Each action is performed upon failure of the previous action.

3.1.10 User and Systems Administrator Notification

All endpoint protection solutions that provide real-time, interactive notification capabilities must be configured to:

- Display a notification to the user and systems administrator upon real-time event detection, and
- Include the action taken in the displayed notification.

Supplemental Information: Separate from systems administrator notification, users should be made aware through automatic notification when malicious code or inappropriate web content is detected and blocked. The purpose of automatic user notification is twofold:

- If the users are unaware that the system is blocking the attempt (for malicious code to run or for an inappropriate site to load), the user may attempt alternate methods that circumvent endpoint protection.
- It alerts the user to contact their ISSO and/or Customer Service Center (CSC) that malicious code has been detected on media.

3.1.11 Endpoint Protection Event Logs

All endpoint protection solutions must be configured to provide attacks or malicious code detection event logs to track the status of all administrative and investigative actions. The event detection related to the endpoint protection must include, at a minimum, the following attributes for post-event analysis and reporting:

- Date/time of detection
- Action taken upon detection
- Name and location of file/website
- Name of device
- Account name (i.e., user account logged on when detection occurred)
- Event content (e.g., port, protocol, source or destination Internet Protocol (IP) address, application, website).

Additional event log collections must be configured in accordance with requirements specified in CSO-STD-2005, as applicable.

3.1.12 Network Interfaces

All endpoint protection solutions must be configured to monitor and protect all network interfaces on endpoints.

Supplemental Information: By design, the latest devices generally have more than one network interface (e.g., a wired and a wireless connection). All endpoint protection solutions should monitor and protect all such interfaces. Leaving an interface unprotected may allow malicious code or other attacks to execute on the system.

3.1.13 Endpoint Encryption

Endpoint protection solutions that support full disk or file-based encryption must be configured to encrypt data for all endpoints.

Supplemental Information: Most EDR solutions offer a way to centrally monitor and manage data encryption on the endpoints (e.g., some EDR solutions can monitor the status of BitLocker, the native encryption tool that comes with Microsoft Windows).

3.1.14 IPv4 and IPv6

All endpoint protection solutions must be configured to apply rulesets for both IPv4 and IPv6 traffic, where applicable.

Supplemental Information: IPv4 and IPv6 traffic is constructed differently at the packet level, and traffic monitoring applications have to be configured specifically to monitor traffic for either protocol. Failure to monitor both protocols may compromise the effectiveness of endpoint protection and may allow undetected reconnaissance or attacks upon the system.

3.1.15 Enable on Startup

All endpoint protection solutions must be configured to enable upon system startup.

Supplemental Information: Failure to monitor the system upon startup compromises the effectiveness of endpoint protection and may allow undetected reconnaissance or attacks.

3.1.16 Prevent Disabling by Non-Privileged User

All endpoint protection solutions that have the capability must be configured to prevent non-privileged users from circumventing endpoint protection capabilities.

3.1.17 Prevent Privilege Escalation

Endpoint protection solutions must not allow executables to execute at higher privilege levels, other than what is specified for each endpoint, as applicable.

3.1.18 Allowlist and Blocklist Updates

Endpoint protection solutions that provide application allowlist and blocklist capabilities must enable automatic updates to the allowlist and blocklist contents.

Supplemental Information: Since executables vary from platform to platform, there is no effective means of manually creating and maintaining a global allowlist for all systems. The automated updates are made available by the trusted publishers (e.g., Palo Alto Cortex XDR) for the antivirus/antimalware files to keep allowlists current to mitigate newer attacks. Therefore, the allowlist for each endpoint has to be maintained dynamically by the application control software.

3.1.19 Semi-Trusted or Restricted Networks, and Disconnected State

All endpoint protection solutions must continue to function when connected to either semi-trusted or restricted networks or working in a disconnected state (i.e., the absence of any network connection).

APPENDIX A. ACRONYMS

ABP	Application Boundary Protection
BYOD	Bring Your Own Device
CSC	Customer Service Center
CSO	Computer Security Organization
EDR	Endpoint Detection and Response
ESA	Enterprise Security Architecture
FIM	File Integrity Monitoring
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
NBP	Network Boundary Protection
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
SGI	Safeguards Information
SSP	System Security Plan
STD	Standard
SUNSI	Sensitive Unclassified Non-Safeguards Information
TRM	Technical Reference Model
WAN	Wide Area Network
XDR	Extended Detection and Response

APPENDIX B. GLOSSARY

Adware	Software that, once downloaded to your endpoint, automatically displays or downloads advertisements on your endpoint.
Allowlist	A list of executable files that is applied in a “deny-all, allow-by-exception.” All executables are prohibited except those which are explicitly allowed by the list.
Antimalware	Software designed to protect endpoints from viruses, worms, Trojan horses, spyware, adware, and other malicious programs.
Antivirus	Software designed to protect endpoints from malicious software.
Blocklist	A list of executable files that is applied in an “allow-all, deny-by-exception.” All executables are allowed to run except those which are explicitly denied by the list.
Botnet	Software designed to infect large numbers of endpoints, causing endpoints to perform automated tasks without the user knowing it (e.g., send out spam email messages, spread viruses, attack endpoints).
Bring Your Own Device	Device (e.g., laptop, smartphone, tablet) not leased or owned by NRC, which NRC has agreed can process sensitive information as long as the user signs an agreement to incorporate specific controls on the device and follow NRC rules regarding processing such information on the device.
Egress	Traffic or commands exiting a device’s network interface.
Endpoint	A remote computing device that is attached to a network, and is capable of sending, receiving, or forwarding information over a communications channel that uses an IP address and port number.
Endpoint Protection	A security approach utilizing system application allowlisting and blocklisting, data integrity monitoring, web content filtering, antimalware protection, host-based NBP, host-based ABP for greater security of endpoints within a system.
Heuristic Analysis	The practice of identifying malware based on previous experiences, observations of malware behavior and typical points of attack.
Host-based Application Boundary Protection	A software package, or component of an endpoint security suite, which monitors a single host for malicious activity, analyzes that activity, logs information about the activity, and attempts to block/stop activity
Host-based Network Boundary Protection	Software-based or hardware-based security tool which controls incoming and outgoing network traffic by analyzing network data packets based on a predetermined ruleset.
Ingress	Traffic or commands coming into a device’s network interface from an external source.
Keylogger	A hardware device or a software program that records the real-time activity of a user including the keyboard keys pressed.

Malicious Code	Software or firmware intended to perform an unauthorized process that has an adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Mobile Desktops	Laptops provided to users by the Office of the Chief Information Officer (OCIO), allowing users to remotely connect to the NRC infrastructure to access NRC resources and process information up to, and including, the Sensitive Unclassified Non-Safeguards Information (SUNSI) level.
Packet	Logical grouping of information that includes a header containing control information and user data.
Real-time Scanning	A capability of antimalware software that operates as a background task, allowing the device to continue working at normal speed, with no perceptible slowing. Examples of real-time scanning occur when files or programs are downloaded to a host endpoint and antivirus software begins to immediately check the file or program for malicious code.
Regional Office LAN	A standalone office LAN located at an NRC regional office.
Rootkit	A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.
Safeguards Information	A special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act to be protected
Semi-trusted Network	Networks where security controls have been applied; limiting risks of system compromise and breaches.
Sensitive Unclassified Non-Safeguards Information	Information that is generally not publicly available and encompasses a wide variety of categories (e.g., personnel privacy, attorney-client privilege, confidential source, etc.).
Spyware	Software that is secretly or surreptitiously installed into a system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Standalone Office LAN	Offices can use a separate standalone LAN located outside the boundaries of the NRC Wide Area Network (WAN). Regional office LANs are considered Standalone Office LANs.
Trojan Horse	A program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.
Trusted Network	A network that employs sufficient hardware and software assurance measures to allow its use for processing Sensitive Unclassified Non-Safeguards Information (SUNSI). For the purposes of this standard, NRC managed networks are the only trusted networks.
User Device Endpoint	A device or the group of devices that are enterprise or independently managed by the NRC (or parties on behalf of the NRC) and form peers for the network connection on LANs.

Virus	A program that can copy itself and infect an endpoint without permission or the knowledge of the user. A virus might corrupt or delete data on a device, use email programs to spread to other devices, or even erase everything on a hard disk.
Worm	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread. See malicious code.

CSO-STD-2108 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
11-Jun-14	1.0	Initial Release	CSO web page	N/A
15-Feb-22	2.0	Revised standard to simplify and update with latest requirements	Post to OCIO/CSO Standards SharePoint Site	N/A