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

Office Instruction:	**CSO-STD-2008**
Office Instruction Title:	**Network Ports, Protocols, and Services Enterprise Security Architecture Standard**
Version Number:	**2.0**
Effective Date:	**September 30, 2020**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-STD-2008, “Network Ports, Protocols, and Services Enterprise Security Architecture Standard,” provides the minimum security requirements that must be met for the use of network ports, protocols, and services on NRC networks or 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 /**	**9/11/20**
CISO	Jonathan Feibus	**/ RA /**	**9/14/20**

TABLE OF CONTENTS

1 PURPOSE 1

2 GENERAL REQUIREMENTS 1

2.1 SYSTEM MONITORING 2
2.2 APPLICABILITY IN CONCERT WITH SECURITY CONFIGURATION BASELINES 2
2.3 RECOMMENDED INTERACTIONS WITH STAKEHOLDERS 2

3 SPECIFIC REQUIREMENTS 2

3.1 NPPS SELECTION 3
3.1.1 Least Functionality 3
3.1.2 Authentication 3
3.1.3 Cryptography 3
3.1.4 Latest Versions 5
3.2 OPERATIONS AND MAINTENANCE REQUIREMENTS 5

APPENDIX A. ACRONYMS 7

APPENDIX B. GLOSSARY 9

APPENDIX C. REFERENCES 10

Computer Security Standard
CSO-STD-2008

Network Ports, Protocols, and Services Enterprise Security Architecture Standard

---

1 PURPOSE

CSO-STD-2008, "Network Ports, Protocols, and Services Enterprise Security Architecture Standard," provides the minimum security requirements for the use of network ports, protocols, and services (NPPS) on Nuclear Regulatory Commission (NRC) networks or systems that store or process information up to, and including, the Safeguards Information (SGI) level.

This standard is intended for system administrators, systems and network architects, information technology (IT) system managers (operational and project-related), system owners, and Information System Security Officers (ISSOs) who must ensure to apply and enforce the NPPS security requirements.

This standard applies to a distinct combination of network services, the protocol(s) used as the transport protocol for the services, and the network port(s) used by the services, to facilitate communications across internal networks, demilitarized zones (DMZ), and external networks.

CSO-STD-2008 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.

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 NPPS used within NRC systems must comply with as the minimum set of controls.

A defense-in-depth approach to NPPS must be employed by maintaining "deny by default" and "allow by exception" rules. Improper use of an NPPS can be the source of system and network compromises.

> For example: The Hypertext Transfer Protocol Secure (HTTPS) service uses the Transmission Control Protocol (TCP) as the transport protocol and is associated with network port 443.

Further details related to NPPS names can be found in the "IANA Service Name and Transport Protocol Port Number Registry."[1]

2.1 System Monitoring

NPPS communication must be monitored in accordance with CSO-STD-2005, "System Monitoring Standard."

2.2 Applicability in Concert with Security Configuration Baselines

The requirements in this standard must be followed unless applicable security configuration baselines[2] provide requirements that conflict with or are in addition to those specified in this standard. In that case, the security configuration baseline requirements take precedence and must be followed.

2.3 Recommended Interactions with Stakeholders

System administrators, system and network architects, IT system managers (operational and project-related), system owners, and ISSOs should work with vendors, integrators, cloud service providers, and NRC colleagues to:

- Review proposed technology solutions/acquisitions to determine if applicable requirements can be met ahead of procurement actions.
- Obtain necessary information on available NPPS for products and configuration/hardening options.
- Plan and implement NPPS within NRC systems and applications to make certain that security requirements are met ahead of production use.

3 SPECIFIC REQUIREMENTS

This section identifies specific requirements applicable to NPPS used within the NRC networks and systems, which may include communication within and between internal networks, DMZs, and external networks. These network types are identified and described in detail within CSO-STD-4000, "Network Infrastructure Standard."

Within a network and system environment, many software packages, network appliances (virtual or physical), and external IT services (e.g., cloud services) automatically install or enable network services as part of their original/default configuration. As a result, unnecessary NPPS increase the possibility for a system to be compromised, which can be due to the lack of security protections (e.g., no protections for data integrity or confidentiality) or a flaw in the

[1] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[2] CSO-PROS-3000, "Cybersecurity Standards Process," specifies how application security configuration baselines (also referred to as "external standards") are identified and apply. These include, but are not restricted to, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Center for Internet Security (CIS) Benchmarks.

NPPS itself that can be exploited by an attacker (e.g., to bypass or weaken controls around authentication).

3.1 NPPS Selection

NRC systems and applications must follow the requirements in the subsections below for the selection/use of necessary, secure, and up-to-date NPPS.

3.1.1 Least Functionality

NPPS must be limited to those that are necessary to support required system functionality.

Explanation: Only use NPPS necessary for required functionality. Many software packages, virtual appliances, and cloud services enable a variety of NPPS by default to facilitate use and integrations. While the initial/default configurations can be helpful for building/developing new applications or systems, these configurations may not be appropriate for production use.

For example:

Many network devices (virtual or physical) may come with multiple Web, file transfer, and command line remote management interfaces enabled. However, if a system only requires an individual Web interface, then the NPPS associated with the file transfer and command line remote management interfaces must be disabled.

3.1.2 Authentication

NPPS that do not require or are not configured to require authentication for remote control, remote access, or the communication of Sensitive Unclassified Non-Safeguards Information (SUNSI) (or Controlled Unclassified Information [CUI]) must not be used.

For example:

The Trivial File Transfer Protocol (TFTP) network service, which uses User Datagram Protocol (UDP) as the transport protocol and listens on port 69, does not require authentication nor does it provide encryption. Therefore, TFTP must not be used for the communication of SUNSI (or CUI).

3.1.3 Cryptography

NPPS are frequently used to communicate SUNSI (or CUI), which have an impact level of Moderate or High. In accordance with CSO-STD-2009, "Cryptographic Control Standard", all NPPS communications involving SUNSI (or CUI) must be encrypted in transit, to protect the confidentiality and integrity of information.[3]

[3] CSO-STD-2009 also states that all sensitive information must be encrypted at rest. The requirements to encrypt data at rest and in transit are mandated per OMB Circular, A-130, "Managing Information as a Strategic Resource."

NRC systems and applications must comply with federal mandates that specify NPPS requirements. The Office of Management and Budget (OMB) Memoranda provide mandates regarding the use of HTTPS and Domain Name System (DNS) NPPS by federal agencies.

Explanation: The following are the federal mandates related to cryptographic requirements for specific NPPS, as referred to above:

- All externally facing NRC websites and services must only be accessible through a securely configured HTTPS connection in accordance with OMB Memorandum (M) M-15-13, "Policy to Require Secure Connections across Federal Websites and Web Services."
- NRC DNS must implement Domain Name System Security Extensions (DNSSEC) in accordance with OMB M-08-23, "Securing the Federal Government's Domain Name System Infrastructure."

For example:

- Network appliances may commonly support insecure methods for remote management, such as the Telnet network service (uses TCP for transport and port 23.) In contrast, a more secure method that uses encryption to protect the confidentiality and integrity of information in transit should be used, such as Secure Shell (SSH).
- A file transfer service, such as the File Transfer Protocol (FTP) (uses TCP for transport and port 21) may be in use by default. This insecure network service should not be used as secure alternatives exist that encrypt data in transit, such as Secure File Transfer Protocol (SFTP).
- Unencrypted Hypertext Transfer Protocol (HTTP) (uses TCP for transport and port 80) has inherent vulnerabilities to confidentiality and integrity that can be mitigated by using HTTPS.

Cryptographic algorithms/ciphers and cipher strengths used within NPPS must be in accordance with CSO-STD-2009, which requires the use of secure, federally validated cryptographic algorithms.

For Example:

- TLS Cipher Suites – Rivest Cipher 4 (RC4) is not approved for federal applications due to an inherent weakness that allows attackers to decrypt the keystream. Similarly, Advanced Encryption Standard (AES) Cipher Block Chaining (CBC) used in TLS version 1.2 or higher is not allowed and has been replaced by a more secure AES Galois/Counter Mode (GCM).
- SSH Cipher Suites – Cast128 and Blowfish (or Twofish) ciphers are commonly enabled by default in various products. Cast128 and Blowfish are both insecure and not permitted for federal use; instead, AES128-Counter (CTR) or AES128-GCM ciphers should be used. AES is a federally approved cryptographic algorithm and CTR and GCM modes do not share vulnerabilities found in other AES encryption modes (e.g., CBC).

3.1.4 Latest Versions

The latest versions of NPPS should be used to take advantage of new security capabilities and security updates to prevent/mitigate the exploitation of vulnerabilities. However, the latest version of an NPPS must be used when the prior version is affected by one or more security vulnerabilities.[4]

For example:

- Version 2.x of the SSH network service is more secure than version 1.x due to inherent security weaknesses in the earlier version that impair data integrity.
- Version 3.0 of the Simple Network Management Protocol (SNMP) network service provides robust authentication methods and protects information in transit while earlier versions of SNMP are known to have significant security weaknesses.
- Version 3.x and version 2.x of Server Message Block (SMB) protocol, that are used by Windows-based computers to allow systems within the same network to share files, are much more secure than the earlier version 1.0. Please note that while both SMB 2.x and 3.x may be used, SMB 3.x provides greater security capabilities.
- Secure Sockets Layer (SSL) 2.0, SSL 3.0, Transport Layer Security (TLS) 1.0, and TLS 1.1 protocols are known to have vulnerabilities (e.g., the Padding Oracle On Downgraded Legacy Encryption [POODLE] cryptographic vulnerability and other cryptographic weaknesses). At the time of the publication of this standard, the latest TLS versions (1.2 and 1.3) are considerably more secure. The TLS protocol and associated use cases are identified in CSO-STD-2009.

3.2 Operations and Maintenance Requirements

The following requirements apply to NPPS within existing NRC systems and those selected per Section 3.1, NPPS Selection (e.g., for new software, servers, or external IT services).

- Any NPPS with known vulnerabilities must be disabled, replaced with a newer version that is not affected by the vulnerabilities, or updated with a patch for the specific vulnerability.
- When new versions of network services associated with NPPS become available, ISSOs and system administrators should plan for timely upgrades/updates to the newest versions. This is especially important when there are known vulnerabilities in the most recent prior version.
- ISSOs and other individuals with cybersecurity responsibilities (e.g., system administrators, engineers, and architects) may use their discretion regarding whether to move to new NPPS versions that do not specifically address a security vulnerability.

---

[4] National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD): An authoritative listing of cybersecurity vulnerabilities, including for NPPS. Vulnerability details include information on affected NPPS, recommended steps for mitigation (e.g., updates to newer versions, configurations), and vendor references. https://nvd.nist.gov/

- Only NPPS that protect data confidentiality and integrity through encryption may be used when crossing different network boundaries/types, such as internal, DMZ, Multiprotocol Label Switching (MPLS)/Wide Area Network (WAN), or Internet, as identified in CSO-STD-4000.

APPENDIX A. ACRONYMS

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CIS	Center for Internet Security
CSO	Computer Security Organization
CTR	Counter
CUI	Controlled Unclassified Information
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
ESA	Enterprise Security Architecture
FISMA	Federal Information Security Modernization Act
FTP	File Transfer Protocol
GCM	Galois/Counter Mode
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
ISSO	Information System Security Officer
IT	Information Technology
M	Memorandum
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
NPPS	Network Ports, Protocols, and Services
NRC	Nuclear Regulatory Commission
NVD	National Vulnerability Database
OMB	Office of Management and Budget
POODLE	Padding Oracle On Downgraded Legacy Encryption
PROS	Process
RC4	Rivest Cipher 4
SFTP	Secure File Transfer Protocol
SGI	Safeguards Information

SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STD	Standard
STIG	Security Technical Implementation Guide
SUNSI	Sensitive Unclassified Non-Safeguards Information
TCP	Transport Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAN	Wide Area Network

APPENDIX B. GLOSSARY

Demilitarized Zone	Perimeter network segment that is logically placed between internal and external networks. Its purpose is to enforce the internal network's information assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from external networks.
Port	Logical connection point used for transmitting information packets.
Protocol	Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.
Service	A named standard or proprietary packet structure that provides the software interface communication from one information network application to another.
Transport Protocol	A network protocol that operates directly on top of network layer protocols, such as Internet Protocol (IP). Transport protocols, such as TCP and UDP, are used by services to ensure reliable and/or fast communication (depending on the transport protocol used).

APPENDIX C. REFERENCES

OMB:

- Circular, A-130, “Managing Information as a Strategic Resource”
- M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure”
- M-15-13, “Policy to Require Secure Connections across Federal Websites and Web Services”

NRC Computer Security Organization (CSO):

- Cybersecurity Issuances

  The following referenced documents are in the CSO Federal Information Security Modernization Act (FISMA) Repository.

  Processes

  https://usnrc.sharepoint.com/:f:/r/teams/OCIO-CSO/CSO_FISMA_Repository/Cybersecurity_Issuances/06_Plan_Procedures_Processes?csf=1&web=1&e=mPtHCd

  - CSO-PROS-3000, “Cybersecurity Standards Process”

  Standards

  https://usnrc.sharepoint.com/:f:/r/teams/OCIO-CSO/CSO_FISMA_Repository/Cybersecurity_Issuances/01_STANDARDS?csf=1&web=1&e=ZtcqLE

  - CSO-STD-2005, “System Monitoring Standard”
  - CSO-STD-2009, “Cryptographic Control Standard”
  - CSO-STD-4000, “Network Infrastructure Standard”

CSO-STD-2008 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
08-Jun-10	1.0	Initial Release	CSO Web page	N/A
14-Sep-20	2.0	Revision to update information on ports, protocols, and services. Standard name changed from “Network Protocol Standard” to “Network Ports, Protocols, and Services Enterprise Security Architecture Standard.”	Post to OCIO/CSO website	Upon request