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

Office Instruction:	**CSO-STD-2009**
Office Instruction Title:	**Cryptographic Control Enterprise Security Architecture Standard**
Version Number:	**3.0**
Effective Date:	**September 15, 2021**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Description:	CSO-STD-2009 “Cryptographic Control Enterprise Security Architecture Standard,” provides the minimum security requirements that must be applied to the Nuclear Regulatory Commission (NRC) systems which utilize cryptographic algorithms, protocols, and cryptographic modules to provide secure communication services.
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/	8/26/2021
CISO (Acting)	Garo Nalabandian	/RA/	9/8/2021

TABLE OF CONTENTS

List of Tables

Computer Security Standard
CSO-STD-2009
Cryptographic Control Enterprise Security Architecture Standard

1 PURPOSE

CSO-STD-2009, "Cryptographic Control Enterprise Security Architecture Standard," provides the minimum security requirements that must be applied to all Nuclear Regulatory Commission (NRC) systems processing information up to, and including, the classified level, that utilize cryptographic algorithms, protocols, or cryptographic modules.

This standard is based on the latest versions of the National Institute of Standards and Technology (NIST) guidance and Federal Information Processing Standards (FIPS) Publications (PUBs), Committee on National Security System (CNSS) issuances, and National Security Agency (NSA) requirements.

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 are responsible to enforce the cryptographic control security requirements.

CSO-STD-2009 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-2009, "Cryptographic Control Enterprise Security Architecture Guidance," which provides further information to facilitate compliance with this standard.

2 GENERAL REQUIREMENTS

This section provides general requirements that all system administrators and ISSOs authorized to administer and configure the cryptographic systems must comply with as the minimum set of controls.

ISSOs must ensure that all national security systems meet CNSS and NSA specified requirements for cryptographic controls. Systems that process Sensitive Compartmented Information (SCI) must adhere to Director of National Intelligence (DNI) policy, standards, and guidance that is provided by the DNI.[1]

[1] DNI – Intelligence Community (IC) Policies and Reports, https://www.dni.gov/index.php/what-we-do/ic-policies-reports.

All externally-facing NRC websites and services must only be accessible through a securely configured Hypertext Transfer Protocol Secure (HTTPS) connection in accordance with the Office of Management and Budget (OMB) Memorandum (M) M-15-13, “Policy to Require Secure Connections across Federal Websites and Web Services.”

All cryptography must be implemented using a FIPS-validated cryptographic module operated in FIPS mode.

NRC must employ a Key Management Infrastructure (KMI) to manage cryptographic modules and keys.

2.1 Cryptographic Algorithms and Modules

The following cryptographic algorithm and module requirements apply to all unclassified systems:

- NRC systems must use FIPS-validated cryptographic algorithms with FIPS-validated modules.
- Only cryptographic modules that meet the following requirements may be used:
  - Maintain a current NIST Cryptographic Module Validation Program (CMVP) validation certificate;
  - Meet all CMVP configuration and policy requirements; and
  - Configuration to support minimum cryptographic strength requirements for the specific application, as specified in Section 3.1, Cryptographic Key Requirements.

Cryptographic algorithms and modules used to protect classified information must comply with the requirements specified by CNSS and NSA for such information.

2.2 Cryptographic Key Management

The following cryptographic key management requirements apply to all unclassified systems:

- Cryptographic key management must comply with NIST Special Publication (SP) 800-57, (all parts, latest revisions):
  - NIST SP 800-57, Part 1, “Recommendation for Kay Management : Part 1 – General”
  - NIST SP 800-57, Part 2, “Recommendation for Key Management: Part 2 – Best Practices for Key Management”
  - NIST SP 800-57, Part 3, “Recommendation for Key Management, Part 3: Application-Specific Key Management”
- Public key certificates must be issued and validated by an NRC-approved Certificate Authority (CA) with an NRC Authorizing Official (AO) authorization to operate (ATO).
- Equipment used to generate, store, and archive cryptographic keys must be physically protected in accordance with NRC Management Directive (MD) 12.5, “NRC Cybersecurity Program.”

Cryptographic key management systems used to protect classified information must comply with the requirements specified by CNSS and NSA for such information.

2.3 Encryption for Data in Transit and at Rest

Classified systems must comply with the encryption of data in transit and data at rest requirements specified by CNSS and NSA.

Unclassified systems must comply with the encryption of data in transit and data at rest requirements specified by OMB Circular A-130, Appendix I, "Responsibilities for Protecting and Managing Federal Information Resources." OMB Circular A-130, Appendix I, provides the following overreaching requirement for encryption of unclassified information in transit and at rest:

> *Encrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information: is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the authorizing official and approved by the agency CIO.*

Cryptographic algorithms and modules, which are used to encrypt data in transit and data at rest to meet the OMB Circular A-130 requirement, must be configured in accordance with Section 3.1, Public and Private Keys, of this standard.

2.4 Transport Layer Security

Use of Transport Layer Security (TLS) 1.0 and 1.1 is disallowed for government-only applications. When interoperability with non-government systems is required, TLS 1.1 and 1.0 may be supported, if configured in accordance with guidelines provided in NIST SP 800-52, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations." NOTE: However, the use of TLS 1.0 or TLS 1.1 is strongly discouraged, unless it is absolutely necessary for interoperability with non-government systems/users.

The following requirements apply to all unclassified NRC information systems employing TLS:

- All implementations and uses of the TLS protocol must meet the minimum requirements specified in NIST SP 800-52.
- Existing NRC systems must use TLS 1.2 at a minimum and should migrate to TLS 1.3 at a priority, as all agencies are required to support TLS 1.3, by January 1, 2024. New system deployments must support TLS 1.3.
- NRC systems must only use NIST-approved TLS cipher suites. NIST-approved cipher suites are specified in NIST SP 800-52.
- NRC systems must be configured to prioritize the strongest TLS cryptographic cipher suite when negotiating a connection between the server and a client. If the client does not support a stronger cipher suite, then another approved cipher suite can be used (with stronger cipher suites prioritized for use over weaker cipher suites).

In addition to NIST requirements, cryptographic algorithms and cipher strengths used for TLS implementations must meet the minimum requirements specified in Sections 3.1, Cryptographic Key Requirements, and 3.2, Public and Private Keys, of this standard.

3 SPECIFIC REQUIREMENTS

This section provides specific requirements for NRC unclassified (not Controlled Unclassified Information [CUI]), CUI Basic and CUI Specified (non-Safeguards Information [SGI]), and CUI Specified (SGI) systems or Sensitive Unclassified Non-Safeguards Information (SUNSI) that utilize cryptographic algorithms, protocols, and cryptographic modules.

All classified information systems must comply with CNSS and NSA specific requirements for cryptographic controls.

3.1 Cryptographic Key Requirements

All cryptographic key sizes and hash functions must comply with the minimum cryptographic strength requirements for the respective NRC system information type as specified in Table 3.1-1, Minimum Cryptographic Strength Requirements.

The following defines the information contained within the columns of Table 3.1-1:

- Information Category: Identifies the sensitivity level of information to encrypt for processing within NRC networks (i.e., unclassified [FIPS 199 low-impact non-CUI], CUI Basic and CUI Specified [non-SGI], or CUI Specified [SGI] or SUNSI).
- Confidentiality and Integrity (High Watermark): Identifies the high watermark impact level of confidentiality or integrity associated with the information type being encrypted (i.e., low, moderate, or high). If the impact level differs between confidentiality and integrity, the higher of the two (high watermark) should be used.
- Minimum Hash (B) HMAC, KMAC: Identifies the minimum Hash-based Message Authentication Code (HMAC) or Keccak-based Message Authentication Code (KMAC) function used in key derivation functions and random bit generation applications.

  For example:

  To exchange CUI Basic and CUI Specified (non-SGI) – Moderate information between a client and server, it can use the HMAC-Secure Hash Algorithm (SHA)1 hash function, at a minimum, to attain the required minimum level of security. However, a higher level of HMAC hash can be used for added security, if so desired.

- Minimum Hash (A) - (Non-HMAC): Identifies hash functions that are used in digital signatures and other applications requiring collision resistance.

  For example:

  To exchange CUI Basic and CUI Specified (non-SGI) – High information between two entities, any one of the listed hash functions can be used (i.e., SHA-256, SHA-512/256, or SHA3-256).

- Minimum Symmetric-Key: Identifies the minimum key size for each information type when symmetric-key algorithm is used for encryption.

- Minimum Asymmetric-Key: Identifies the key type and the associated length/size to use for encrypting each information type.

  For example:

  An RSA-3072 key, coupled with hash function SHA-384, provides computation of a digital signature that can be used to process a CUI Specified (SGI) information type.

Table 3.1-1: Minimum Cryptographic Strength Requirements

Information Category	Confidentiality and Integrity (High Watermark)	Minimum Hash (B) (HMAC, KMAC)	Minimum Hash (A) (Non-HMAC)	Minimum Symmetric-Key	Minimum Asymmetric-Key
Unclassified (non-CUI)					
Unclassified (non-CUI)	Low	SHA1	SHA-224 SHA-512/224 SHA3-224	128-bit AES	DSA – 2048 bits RSA – 2048 bits DH Group 14 – 2048 bits EC – 224 bits
CUI Basic and CUI Specified (non-SGI) / SUNSI					
CUI Basic & CUI Specified (non-SGI) **/** SUNSI	Moderate	SHA1 KMAC128	SHA-256 SHA-512/224 SHA3-256	128-bit AES (GCM – mode)	DSA – 2048 bits RSA – 2048 bits DH/MQV Group 14 – 2048 bits EC – 256 bits
CUI Specified (non-SGI) **/** SUNSI	High	SHA1 KMAC128	SHA-256 SHA-512/256 SHA3-256	128-bit AES (GCM – mode)	DSA – 2048 bits RSA – 2048 bits DH/MQV Group 14 – 2048 bits EC – 256 bits
CUI Specified (SGI) / SUNSI					
CUI Specified (SGI) **/** SUNSI	High	SHA-256 KMAC256	SHA-384 SHA3-384	256-bit AES	DSA – 3072 bits RSA – 3072 bits DH/MQV Group 15 – 3072 bits EC – 384 bits

It is recommended that stronger cryptographic algorithms and cipher strength are used, if possible. Refer to CSO-GUID-2009, Section 2.5, Cryptographic Algorithms and Security Strength, for further information on greater security provided by the algorithms and security strength options.

3.2 Public and Private Keys

NRC systems or applications must have separate public certificates and key pairs for authentication and for encryption. The private key for authentication should never be known to anyone other than the owner of that key pair. The key pair owner can be any entity (for example, a user, a system owner, or designated key pair holder) depending on the system and specific implementation.

While creating digital certificates and key pairs for protection of data:

- The digital signature certificate and key pairs must only be used for identification and authentication.

- The encryption certificate and key pairs must only be used for purposes of encryption.
- The certificates and associated key pairs used to access or encrypt CUI Specified (SGI)/ SUNSI (high) applications must be kept separate and distinct from certificates and associated key pairs used in CUI Basic/CUI Specified (non-SGI)/SUNSI (moderate) applications or applications/systems using non-public/non-sensitive and public information.
- All encryption certificates must be issued by an NRC CA that has received an ATO by the NRC AO (e.g., enterprise NRC ICAM public and private CAs).
- Self-signed certificates must not be used in any NRC system.

The private key for encryption should be placed in a key escrow to enable decryption of information if the key pair owner is not available. Escrowed encryption private keys should be under a two-person rule (i.e., requires the presence of two authorized individuals at the same time to access the key) with established procedures to ensure the keys are made available only for NRC authorized purposes.

3.3 Cryptographic Key Management

The following requirements apply to cryptographic key management:

- An AO authorized Key Management solution must be used to generate cryptographic keys (e.g., for digital signatures) within NRC systems. This does include OCIO private CA and external, public CA as examples of AO authorized solutions.
- A cryptoperiod (key lifetime designation) must:
  - Be assigned to a key upon key issuance.
  - Be determined based on the categorization of data being encrypted, key strength, and risk factors.
  - Meet the guidelines provided in NIST SP 800-57 (all parts).
  - Be used to either replace or destroy the keys, as applicable.

APPENDIX A. ACRONYMS

AES	Advanced Encryption Standard
AO	Authorizing Official
ATO	Authorization to Operate
CA	Certificate Authority
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CSO	Computer Security Organization
CUI	Controlled Unclassified Information
DH	Diffie-Hellman Key Exchange
DNI	Director of National Intelligence
DSA	Digital Signature Algorithm
EA	Executive Agent
EC	Elliptic Curve
ESA	Enterprise Security Architecture
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GUID	Guidance
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IC	Intelligence Community
ISSO	Information System Security Officer
IT	Information Technology
KMAC	Keccak-based Message Authentication Code
KMI	Key Management Infrastructure
M	Memorandum
MAC	Message Authentication Code
MD	Management Directive
MQV	Menezes-Qu-Vanstone
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
OCIO	Office of the Chief Information Officer
OMB	Office of Management & Budget

PKI	Public Key Infrastructure
PUB	Publication
RSA	Rivest-Shamir- Adleman
SCI	Sensitive Compartmented Information
SGI	Safeguards Information
SHA	Secure Hash Algorithm
SP	Special Publication
STD	Standard
SUNSI	Sensitive Unclassified Non-Safeguards Information
TLS	Transport Layer Security

APPENDIX B. GLOSSARY

Approved	FIPS or NIST approved. An algorithm or technique that is either: • Specified in a FIPS PUB or NIST SP, or • Adopted in a FIPS PUB or NIST SP.
Bits of Security	A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system. The security strength is specified in bits and is a specific value from the set (80, 112, 128, 192, and 256). Note that a security strength of 80 bits is no longer considered sufficiently secure.
Certificate	A set of data that uniquely identifies a key pair and an owner that is authorized to use the key pair. The certificate contains the owner's public key and possibly other information, and is digitally signed by a CA (i.e., a trusted party), thereby binding the public key to the owner.
Certification Authority	The entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates and exacting compliance with a PKI policy.
Ciphertext	Data in its encrypted form.
Cryptographic Algorithm	A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output.
Cryptographic Boundary	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all hardware, software, and/or firmware components of a cryptographic module.
Cryptographic Key	A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.
Cryptographic Module	The set of hardware, software, and/or firmware that implements at least one approved security function (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Cryptographic System	Associated information security items interacting to provide a single means of encryption or decryption.
Cryptoperiod	The time span during which a specific key is authorized for use or remains in effect for a given system or application.

CUI	Federal Register 32 Code of Federal Regulations (CFR) Part 2002, “Controlled Unclassified Information; Final Rule,” established policy for a federal government-wide CUI program and a CUI Registry, maintained by the CUI Executive Agent (EA), to provide authorized categories, subcategories, associated markings, as well as applicable safeguarding, dissemination, and decontrol procedures for CUI. The CUI program provides a standardized and simplified way to manage unclassified information that requires protections and dissemination controls, pursuant to and consistent with applicable laws, regulations, and government-wide policies. This excludes all information classified under EO 13526, “Classified National Security Information,” dated December 29, 2009, and the Atomic Energy Act of 1954, as amended. All federal government-wide unclassified information that requires any protection or dissemination control is declared CUI and mandates that authorized holders protect CUI using CUI Basic or CUI Specified controls.
CUI Basic	CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic per the uniform set of controls in the 32 CFR Part 2002 and the CUI Registry. All CUI Basic categories are controlled at ‘moderate’ confidentiality level at a minimum. However, some CUI may have higher, or different level of requirements if a law, regulation, or government-wide policy requires or permits other controls for protecting or disseminating that information. The final rule mandates that authorized holders of CUI use at least the CUI Basic default set of standards to protect information.
CUI Specified	CUI Specified is the subset of CUI in which the authorizing law, regulation, or government-wide policy contains specific handling controls that it requires or permits agencies to use that are in addition to those for CUI Basic. The CUI Registry indicates which laws, regulations, and government-wide policies include such specific requirements. CUI Specified information may be handled at higher confidentiality levels if the authorities establishing and governing the CUI Specified allow or require a more specific or stringent controls. SGI is considered to be CUI specified and requires more stringent controls.
Decryption	The process of transforming ciphertext into plaintext using a cryptographic algorithm and key.
Digital Signature	The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation.
Encryption	The cryptographic transformation of data to produce ciphertext.
Entity	A person, organization, device, or process.
Hash Function	A mathematical function that maps a string of arbitrary length (up to a predetermined maximum size) to a fixed length string.
Hash-based Message Authentication Code	A message authentication code that utilizes a keyed hash.

Key	A parameter used in conjunction with a cryptographic algorithm that determines its operation.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.
Key Management Infrastructure	The framework and services that provide the generation, production, storage, protection, distribution, control, tracking, and destruction for all cryptographic keying material, symmetric keys as well as public keys and public key certificates.
Key Pair	A public key and its corresponding private key.
Key-Derivation Function	A function that generates a binary string, called keying material, with the input of a cryptographic key or shared secret and possibly other data.
Keying Material	The data necessary to establish and maintain cryptographic keying relationships.
Message	The data that is signed. Also known as “signed data” during the signature verification and validation process.
Message Authentication Code	A cryptographic checksum that results from passing data through a message authentication algorithm. In this standard, the message authentication algorithm is called HMAC, while the result of applying HMAC is called the Message Authentication Code (MAC).
Private Key	A cryptographic key that is used with an asymmetric cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key.
Public Key	A cryptographic key that is used with an asymmetric cryptographic algorithm and is associated with a private key. The public key is associated with an owner and may be made public. In the case of digital signatures, the public key is used to verify a digital signature that was signed using the corresponding private key.
Secret Key	A cryptographic key that is uniquely associated with one or more entities. The use of the term "secret" in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.
Security Strength	A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system. Sometimes referred to as a security level or bits of security.

Self-Signed Certificate	A public-key certificate whose digital signature may be verified by the public key contained within the certificate. The signature on a self-signed certificate protects the integrity of the data, but does not guarantee the authenticity of the information. The trust of self-signed certificates is based on the secure procedures used to distribute them.
Signatory	The entity that generates a digital signature on data using a private key.
Static Key	A key that is intended for use for a long period of time and is for use in many instances of cryptographic key-establishment schemes.
Symmetric-Key	A cryptographic algorithm that uses the same secret key for an operation; such as encryption and decryption.

CSO-STD-2009 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 ISD web page	Upon request
05-Sep-17	2.0	Revised based on the latest versions of NIST PUBs and FIPS PUBs addressing cryptographic controls based upon the current threat environment.	Distribution at ISSO forum and posting on OCIO web page	Upon request
08-Sep-21	3.0	Revised based on the latest versions of NIST SPs and FIPS PUBs addressing cryptographic controls based upon the current threat environment.	Post to OCIO/CSO Standards SharePoint Site	Upon request