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

Office Instruction:	**OCIO-CS-PROS-2001**
Office Instruction Title:	**System Security Categorization Process**
Revision Number:	**1.1**
Issuance Date:	**Date of last signature below**
Effective Date:	**Upon Issuance**
Primary Contacts:	**Kathy Lyons-Burke, Senior Level Advisor for Information Security**
Responsible Organization:	**OCIO**
Summary of Changes:	OCIO-CS-PROS-2001, “System Security Categorization Process” defines the process that must be followed to determine the security categorization and e-authentication requirements for NRC information and systems.
Training:	As needed
ADAMS Accession No.:	ML17067A218

Approvals			
Primary Office Owner	Office of the Chief Information Officer	**Signature**	**Date**
Chief Information Officer	David Nelson	/RA/	03/27/2017
Chief Information Security Officer	Jon Feibus, acting	/RA/	02/27/2017

Table of Contents

1 Purpose 1

2 General Requirements 1

2.1 Definitions 2

2.2 Required Information 5

2.3 Outputs 7

2.4 References 8

3 Determine Security Categorization 8

3.1 Determine Information Types 9

3.2 Determine Information Sensitivity 10

3.3 Document Security Categorization 11

4 Determine E-Authentication Requirements 11

4.1 Identify Open Network Transactions 12

4.2 Assess E-Authentication Risk 12

4.3 Determine Required Assurance Level 14

4.4 Document E-Authentication Risk Assessment 15

5 Submit Security Categorization Report 15

Appendix A Acronyms 16

Appendix B NRC Information Types and Sensitivity 18

Computer Security Process
OCIO-CS-PROS-2001

System Cybersecurity Control Independent Assessment Frequencies Process

1 PURPOSE

OCIO-CS-PROS-2001, System Security Categorization Process is the process that must be followed to determine the security categorization and e-authentication requirements for NRC unclassified information and systems. This information is documented in a security categorization report. The results of this process are used to determine the required cybersecurity controls for the system as well as the level of authentication required for publicly accessible authenticated transactions.

The information in this document is intended to be used by system owners, information owners, information system security officers (ISSOs), and cybersecurity oversight personnel.

2 GENERAL REQUIREMENTS

Federal agencies are required to determine the sensitivity of the information that is processed, stored, or transmitted by their systems. This determination is specifically identified in Federal Information Processing Standard (FIPS) 199, “Standards for Security Categorization of Federal Information and Information Systems.” Use of this standard applies to all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and to all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2).

System owners must ensure that this process is used to categorize all information processed, stored, or transmitted by their systems, as well as for NRC information processed, stored, or transmitted by another agency system that NRC has authorized to operate for NRC purposes.

The categorization is based on the potential impact that a compromise to the confidentiality, integrity, or availability of information could produce. This categorization does not take into account any controls, but rather poses the question of what is the worst that could happen if the information is available to those that should not have it, if the information is modified to an unauthorized value or deleted, or if the information is not available when it is needed. These impacts can be to mission functions, financial stability, the public, the Nuclear Regulatory Commission’s (NRC’s) reputation, etc.

Complex systems must be broken down into subsystems so the systems can be fully understood and managed. Higher sensitivity information should be isolated to specific subsystems to enable better protection of the information and reduce implementation of greater security controls across the enterprise. Subsystems should contain assets that use the same information types.

If the system is public-facing, a detailed transaction analysis must be conducted in accordance with Office of Management and Budget (OMB) Memorandum 04-04 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, "Electronic Authentication Guideline" in order to ensure that authentication processes provide the appropriate level of assurance.

The results of this process are documented in a security categorization report in accordance with CSO-TEMP-2001, "System Security Categorization Report."

2.1 Definitions

Availability

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of availability is the disruption of access to or use of information or an information system

At the NRC, the following timeframes are used for availability:

- Low availability: the system/information shall not be unavailable for longer than 30 calendar days.
- Moderate 1 availability: the system/information shall not be unavailability for longer than 14 calendar days.
- Moderate 2 availability: the system/information shall not be unavailability for longer than 2 business days.
- High availability: the system/information shall not be unavailability for longer than 12 calendar hours.

Selection of moderate availability 1 or 2 depends upon the business needs for the system/information.

Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of confidentiality is the unauthorized disclosure of information.

Controlled Unclassified Information (CUI)

Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a nonexecutive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. [32 CFR Part 2002]

Credential

An object that is verified when presented to the verifier in an authentication transaction. [OMB M-04-04]

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 according to the uniform set of controls set forth in this part and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified in this section), and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI. [32 CFR Part 2002]

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 differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance. [32 CFR Part 2002]

FedRAMP

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), NIST, Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), OMB, the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

HIGH potential impact

The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

High watermark

The highest value of sensitivity across all information types stored on, processed by, or transiting the system.

Information owner

An information owner is an office director, regional administrator, or OCIO division director that has overall responsibility for protecting a particular type of information that is electronically processed, stored, or transmitted by a system owned by or operated on behalf of NRC. An information owner provides requirements to IT system owners regarding the security controls for the IT systems where the information resides. The information owner is an agency official who has inherent U.S. Government authority and must be a Government employee.

Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of integrity is the unauthorized modification or destruction of information.

LOW potential impact

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

MODERATE potential impact

The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Subsystem
A subsystem is a part of a system that has a defined boundary with defined functionality and a subsystem owner.

System owner
A system owner is an office director, regional administrator, or OCIO division director that has overall responsibility for the security of NRC systems owned by his or her organization or operated on behalf of his or her organization by another agency or by a contractor. The system owner is an agency official who has inherent U.S. Government authority and must be a Government employee.

Transaction
A discrete event between user and systems that supports a business or programmatic purpose. [OMB M-04-04]

Uncontrolled unclassified information
Information that neither the Order nor the authorities governing classified information cover as protected. Although this information is not controlled or classified, agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements. [32 CFR Part 2002]

2.2 Required Information

This process is used at three different points in the system life-cycle: new systems, system security categorization and e-authentication revalidation, and system changes. New system security categorizations and e-authentication requirements must be prepared at project initiation before system design. System security categorization and e-authentication requirements revalidation occur for new systems just prior to system authorization and periodically (e.g., annually) thereafter. System security categorization and e-authentication requirements update or revalidation must also be performed prior to system change implementation. Both the security categorization and the e-authentication requirements identification are documented in the security categorization report. The timing for the documentation as shown in Table 1.

Table 1: Security Categorization Report Timeframes

System Timeframe	Required Documentation
Project Initiation	Preliminary Security Categorization Report
Immediately prior to new system deployment	Final Security Categorization Report
Immediately prior to system change deployment	Updated Security Categorization Report
Change in NRC information types	Verified Security Categorization Report

Table 2 identifies the information that is required in order to begin this process.

Table 2: Information Required to Begin Security Categorization and E-Authentication Requirement Determination

Information	New Systems	System Security Categorization Validation and System Changes
System name	The formal name of the FISMA reportable system.	

Table 2: Information Required to Begin Security Categorization and E-Authentication Requirement Determination

Information	New Systems	System Security Categorization Validation and System Changes
System description	A system description provides a high-level description of the system, its functions, and its mission objective. This description elaborates on how the system relates to the mission or objectives to the owning organization and to the agency, and includes a description of the physical operating environment for the system (site locations, high-level server room description, and key physical and environmental security features of server rooms). The system description also indicates whether the system is a cloud implementation, owned or operated by another federal agency, contractor hosted and operated, or a FedRAMP system.	
System owner identity	The organizational position of the NRC system owner (e.g., Director, Office of Administration).	
System ISSO	The identity of the system ISSO.	
Subsystem ISSO*	The identity of the subsystem ISSO.	
Subsystem names*	The formal name of a subsystem within the FISMA reportable system.	
Subsystem description*	A subsystem description provides a high-level description of the subsystem, its functions, and its mission objective. This description elaborates on how the subsystem relates to the mission or objectives to the owning organization and to the agency, and includes a description of the physical operating environment for the subsystem (site locations, high-level server room description, and key physical and environmental security features of server rooms). The subsystem description also indicates whether the subsystem is a cloud implementation, owned or operated by another federal agency, contractor hosted and operated, or a FedRAMP system.	
System boundary	A system context diagram and description that clearly (to the extent known): • indicate physical locations of components • identify all interfaces external to the system • identify all interfaces with organizations external to the NRC	A system diagram and description that clearly: • define the hardware and software that constitute the FISMA reportable system • indicate physical locations of components • identify all interfaces external to the system • identify all interfaces with organizations external to the NRC
Subsystem boundary*	A subsystem context diagram and description that clearly (to the extent known): • indicate physical locations of components • identify all interfaces external to the subsystem • identify all interfaces with organizations external to the NRC	A subsystem diagram and description that clearly: • define the hardware and software that constitute the FISMA reportable subsystem • indicate physical locations of components • identify all interfaces external to the subsystem

Table 2: Information Required to Begin Security Categorization and E-Authentication Requirement Determination

Information	New Systems	System Security Categorization Validation and System Changes
		• identify all interfaces with organizations external to the NRC
System information	An initial list of information stored on, processed by, or transiting the system.	A list of information stored on, processed by, or transiting the system.
Subsystem information*	An initial list of information stored on, processed by, or transiting the subsystem.	A list of information stored on, processed by, or transiting the subsystem.
Information owner identities	The organizational position of the NRC information owner (e.g., Director, Office of Administration) for each type of information.	
Privacy Threshold Analysis and/or Privacy Impact Assessment	An initial indication of privacy information that may be processed, stored, or transmitted by the system.	Privacy impact analysis is required by the Privacy Act. A Privacy Threshold Analysis (PTA) is used to determine whether a Privacy Impact Assessment (PIA) is needed. Some systems will not require a PIA if the system will not collect, maintain, or disseminate information about individuals. If a PIA is not required, the system should have a PTA on file documenting this determination. The PTA template can be found in ADAMS (ML091970114). If the PTA determines that the system processes information about individuals (including members of the public), a PIA must be performed.
System/subsystem risk assessment	An initial system risk assessment document identifying the risk associated with the system at a high level.	A system risk assessment document where the risk assessment was performed in accordance with NIST SP 800-30.

*If applicable

2.3 Outputs

Table 3 identifies the outputs from this process.

Table 3: Security Categorization and E-Authentication Requirement Determination Outputs

Output	Description
System security categorization	A determination of the system confidentiality, integrity, and availability sensitivity performed in accordance with FIPS 199.
Subsystem security categorization*	A determination of the subsystem confidentiality, integrity, and availability sensitivity performed in accordance with FIPS 199.
System E-Authentication Risk Assessment	A determination of the level of authentication required for each system transaction with the public performed in accordance with M-04-04.

Table 3: Security Categorization and E-Authentication Requirement Determination Outputs

Output	Description
Subsystem E-Authentication Risk Assessment*	A determination of the level of authentication required for each subsystem transaction with the public performed in accordance with M-04-04.
System Security Categorization Report	The system security categorization and e-authentication requirements documented in accordance with CSO-TEMP-2001.

*If applicable

2.4 References

The following references were used to develop this process:

- 32 CFR Part 2002, Controlled Unclassified Information
- CSO-TEMP-2001, “System Security Categorization Report”
- Federal Information Security Modernization Act (FISMA) of 2014
- FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems”
- FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems”
- NIST SP 800-30, “Guide for Conducting Risk Assessments”
- NIST SP 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”
- NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”
- NIST SP 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories”
- NIST SP 800-63, “Electronic Authentication Guideline”
- OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies”

3 DETERMINE SECURITY CATEGORIZATION

Security categories are determined for both information and systems and are based upon the potential impact of compromise of the confidentiality, integrity, and availability of the information and the system. Security categories provide input to the risk assessment process and are used with vulnerability and threat information to identify system and information risk.

The security categorization process involves the following steps:

- Identifying the information types that are stored, processed, or transmitted by the system, using the defined system boundaries.

- Identifying the high-water mark (highest value identified) for each of the confidentiality, integrity, and availability aspects of information sensitivity.
- Documenting the information sensitivity and system sensitivity in a security categorization report.

3.1 Determine Information Types

Federal Information Processing Standards (FIPS) 199 require agencies to identify all of the applicable information types that are representative of input, stored, processed, and/or output data from each system. The identification of information processed on an information system is essential for the proper selection of security controls and ensuring the confidentiality, integrity, and availability of the system and its information. Determining the security category of an information system requires more analysis and must consider the security categories of all information types resident on the information system.

Appendix B provides the information types and sensitivity levels for NRC information currently identified by NRC information owners. The ISSO uses Appendix B to identify the information types processed by, stored on, or transmitted by the system/subsystem. If an information type has been identified that is not included in this appendix, the NRC CIO and Chief Information Security Officer (CISO) should be notified to enable updating the list of NRC information types, if appropriate. The table below is reproduced from FIPS 199 for reference.

Security Objective	**POTENTIAL IMPACT**		
	LOW	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to	The disruption of access to or use of information or an information system could be expected to	The disruption of access to or use of information or an information system could be expected to

Security Objective	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
[44 U.S.C., SEC. 3542]	have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

3.2 Determine Information Sensitivity

The security categories are based on the potential impact on an organization, the public, and the nation should certain events occur. The potential impacts could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The consequences or impact of unauthorized disclosure of information, modification or destruction of information, and disruption of access to or use of information are defined by the nature and beneficiary of the service being provided or supported.

FIPS 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems for each of three stated security objectives (confidentiality, integrity, and availability).

The default information sensitivity of NRC information has been determined by NRC information owners as documented in Appendix B. In order to determine the sensitivity of the information in the system/subsystem, the ISSO and system owner should use the sensitivities identified in Appendix B as the minimum values for NRC (exceptions can apply for integrity and availability). The special circumstances surrounding the system and the processing of the information on the system may dictate other sensitivities that are higher than those identified in Appendix B. If there are special circumstances that require a different sensitivity level, the NRC information owner, CIO, and CISO should be notified to enable updating the list of NRC information types, if appropriate.

The ISSO summarizes the sensitivity levels across each subsystem (if applicable) and across the system. The high water mark is used to determine the system and subsystem security categorizations. This is accomplished using the following steps for each subsystem and overall system:

1. Review identified security categorizations for the aggregate of information types. Determine the system security categorization (SC) by identifying the security impact level high watermark for each of the security objectives (confidentiality, integrity, availability):

   SC System X = {(confidentiality, impact), (integrity, impact), (availability, impact)}

2. Assign the overall information impact level based on the highest impact level across the system security objectives (confidentiality, integrity, availability)

For example, if a subsystem has the following information type sensitivity:

Information Type	Confidentiality Sensitivity	Integrity Sensitivity	Availability Sensitivity
A	Low	Low	Low
B	Low	Low	Low
C	High	Moderate	Low
D	Low	Low	Low

Then the resulting subsystem security categorization would be:

SC Subsystem X = {(confidentiality, High), (integrity, Moderate), (availability, Low)}

3.3 Document Security Categorization

The system ISSO must document the information types, their sensitivity, and the subsystem/system security categorization in CSO-TEMP-2001 and obtain concurrence on the documented security categorization from the system owner and the information security branch chief, and if the values were modified from those in Appendix B, from the information owner.

4 DETERMINE E-AUTHENTICATION REQUIREMENTS

All agencies must review new and existing electronic transactions that take place over an open network (e.g., Internet) to ensure that authentication processes provide the appropriate level of assurance. There are four levels of identity assurance for electronic transactions requiring authentication:

Level 1	Little or no confidence in the asserted identity's validity.
Level 2	Some confidence in the asserted identity's validity.
Level 3	High confidence in the asserted identity's validity.
Level 4	Very high confidence in the asserted identity's validity.

Authentication focuses on confirming a person's identity, based on the reliability of his or her credential.

In order to successfully implement a government service electronically (or e-government), Federal agencies must determine the required level of assurance in the authentication for each transaction. This is accomplished through a risk assessment for each transaction. The assessment identifies:

a. risks, and
b. their likelihood of occurrence.

The e-authentication requirements identification process involves the following steps:

1. Identifying the system/subsystem transactions that occur over an open network.
2. Assessing the e-authentication risk associated with the transactions that occur over an open network.

3. Determining the required assurance level for each transaction.
4. Documenting the e-authentication risk assessment in a security categorization report.

4.1 Identify Open Network Transactions

The ISSO first determines if an e-authentication risk assessment is required for the system by determining the answer to the following questions:

- Does the system require authentication?
- Is the system browser based or accessed using the Internet?
- Is the system external facing (with external users requiring authentication)?

If the answer to any of the questions is "no", then an e-authentication risk assessment is not required for this system. If the answers are all "yes," the ISSO identifies all transactions that occur over an open network. These transactions may include transactions performed by NRC intranet users when they are accessing resources remotely.

4.2 Assess E-Authentication Risk

Not all Federal electronic transactions over an open network require authentication. For those transactions that require authentication, there are two types of individual authentication:

a. Identity authentication: confirming a person's unique identity.
b. Attribute authentication: confirming that the person belongs to a particular group (such as military veterans or U.S. citizens).

Attribute authentication is the process of establishing an understood level of confidence that an individual possesses a specific attribute. If the attribute does not provide ties to the user's identity; the credential is considered to be an anonymous credential.

Required assurance levels for electronic transactions are determined by assessing the potential harm for each of the above categories. If authentication errors cause no measurable consequences for a category, there is "no" impact. The ISSO determines the potential impact of authentication errors in accordance with Table 4.

Table 4: Potential Harm of Transaction Authentication Errors

Impact Category	Low	Moderate	High
Potential impact of inconvenience, distress, or damage to standing or reputation:	At worst, limited, short-term inconvenience, distress or embarrassment to any party.	At worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.	Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).
Potential impact of financial loss:	At worst, an insignificant or inconsequential	At worst, a serious unrecoverable financial	Severe or catastrophic unrecoverable financial

Table 4: Potential Harm of Transaction Authentication Errors

Impact Category	Low	Moderate	High
	unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.	loss to any party, or a serious agency liability.	loss to any party; or severe or catastrophic agency liability
Potential impact of harm to agency programs or public interests:	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.	At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.
Potential impact of unauthorized release of sensitive information:	At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.	At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199	A release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.
Potential impact to personal safety:	At worst, minor injury not requiring medical treatment.	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.	A risk of serious injury or death.
The potential impact of civil or criminal violations is:	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.	A risk of civil or criminal violations that are of special importance to enforcement programs.

In analyzing potential risks, all of the potential direct and indirect results of an authentication failure must be considered, including the possibility that there will be more than one failure, or harms to more than one person. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The context and the nature of the persons or entities affected should be considered to decide the relative significance of these harms.

4.3 Determine Required Assurance Level

The ISSO compares the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table 5. The ISSO determines the required assurance level by finding the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment.

Table 5: Maximum Potential Impacts for Each Assurance Level

Potential Impact Categories for Authentication Errors	**Assurance Level Impact Profiles**			
	1	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	N/A	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

In some cases, impact may correspond to multiple assurance levels. For example, Table 5 shows that a moderate risk of financial loss corresponds to assurance levels 2 and 3. In such cases, the ISSO uses the context to determine the appropriate assurance level. The assurance level is determined using the following steps:

1. Use the system/subsystem risk assessment of the e-government system to identify the relative severity of the potential harm and likelihood of occurrence of a wide range of impacts (to any party) associated with the e-government system in the event of an identity authentication error.
2. Map identified risks to the required assurance level.

   To determine the required assurance level, initially identify risks inherent in the transaction process, regardless of its authentication technology. Then tie the potential impact category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of potential impacts identified. Thus, if five categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a Level 2 authentication. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, map to the risk profile identified under Level 4, even if other consequences are minimal.

3. Select technology based on the NIST e-authentication technical guidance. After determining the assurance level, refer to NIST SP 800-63 to identify and implement the appropriate technical requirements.
4. After implementation, validate that the information system has operationally achieved the required assurance level. Because some implementations may create or compound particular risks, conduct a final validation to confirm that the system achieves the

required assurance level for the user-to-agency process. The agency should validate that the authentication process satisfies the system's authentication requirements as part of required security procedures (e.g., system authorization).

5. Periodically reassess the information system to determine technology refresh requirements. The agency must periodically reassess the information system to ensure that the identity authentication requirements continue to be valid as a result of technology changes or changes to the agency's business processes. Annual information security assessment requirements provide an excellent opportunity for this. Agencies may adjust the identity credential's level of assurance using additional risk mitigation measures. Easing identity credential assurance level requirements may increase the size of the enabled customer pool, but agencies must ensure that this does not corrupt the system's choice of the appropriate assurance level.

4.4 Document E-Authentication Risk Assessment

The system ISSO must document the e-authentication risk assessment in CSO-TEMP-2001 and obtain concurrence on the documented e-authentication levels from the system owner and the information security branch chief.

5 SUBMIT SECURITY CATEGORIZATION REPORT

Once the security categorization report has been concurred upon by the information owners and the OCIO information security branch chief and approved by the system ISSO and system owner, the report is declared an official agency record and provided to the CISO and the OCIO Information Security Branch Chief, preferably via email, using the Agencywide Documents Access and Management System (ADAMS) accession number of the report.

APPENDIX A ACRONYMS

ACCESS	Automated Access Control and Computer Enhanced Security System
ACS	Authentication and Credentialing Services
ADAMS	Agencywide Documents Access and Management System
CFR	Code of Federal Regulations
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DOD	Department of Defense
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act of 2014
GSA	General Services Administration
ISSO	Information System Security Officers
LAN	Local Area Network
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PIV	Personal Identity Verification
PTA	Privacy Threshold Analysis
SC	Security Categorization
SGI	Safeguards Information

SP	Special Publication
SQL	Structured Query Language
USC	United States Code

APPENDIX B NRC INFORMATION TYPES AND SENSITIVITY

Controls based upon the information sensitivity apply to the entire system lifecycle. Sensitivity of an information type sometimes depends upon the sensitivity of the information that information type references. For example, if there is a vulnerability in a system, the information regarding that vulnerability is considered as sensitive as the most sensitive information that could be accessed if the system was compromised. Another example is the sensitivity of incident response information. Incident response information is at the same sensitivity as the information that could be compromised as part of the incident.

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
Rulemaking and Guidance	Rulemaking and guidance documents, public	Yes	N/A	C.2.2 Regulatory Development (all subtypes)	L	L	L	Consistent with NIST guidance provisional security categorization, with Confidentiality increased to M for CUI, including draft information.	All
Rulemaking and Guidance	Rulemaking and guidance documents, non-public, including CUI that is not SGI	No	Nuclear: Security-Related Information (NRC RIS 2005-31) Specified		M	L	L		
Licensing/ Certification	Applications, RAIs, licenses, certificates, public	Yes	N/A	D.21.3 Permits and Licensing	L	L	L	Consistent with NIST guidance provisional security categorization, with Confidentiality increased to M for CUI, including draft information.	NRR, NMSS, NRO, NSIR, OIP
Licensing/ Certification	Applications, RAIs, licenses, certificates, non-public, including CUI that is not SGI	No	Proprietary Business Information: Manufacturer (15 USC 2055(b)) Basic; Nuclear: Security-Related Information (NRC RIS 2005-31) Specified		M	L	L		
Inspection	Inspection reports, public	Yes	N/A	D.21.1 Inspections and Auditing	L	L	L	NIST guidance provisional security categorization is MML for non-public, however, this is based on presumptions that are not credible in our regulatory regime (e.g., that licensees will penetrate our systems to gain intelligence to enable themselves to	NRR, NMSS, NRO, NSIR, OIP
Inspection	Inspection reports, non-public, including CUI that is not SGI	No	Critical Infrastructure: Critical Infrastructure-Critical Energy Infrastructure Information (18 CFR 388.113), Basic		M	L	L		
Enforcement	Notices of violation, civil penalties	Yes	N/A		L	L	L		

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
Enforcement	Notices of violation, civil penalties, non-public, including CUI that is not SGI	No	Critical Infrastructure: Critical Infrastructure-Critical Energy Infrastructure Information (18 CFR 388.113), Basic		M	L	L	circumvent our inspection programs or to change inspection results)	
Allegations	Correspondence (letters, emails), public (rare)	Yes	N/A	D.21.1 Inspections and Auditing	L	L	L	NIST guidance provisional security categorization is MML for non-public, however, this is based on presumptions that are not credible in our regulatory regime (e.g., that licensees will penetrate our systems to gain intelligence to enable themselves to circumvent our inspection programs or to change inspection results)	
Allegations	Correspondence (letters, emails), internal documentation/tracking, non-public, including CUI that is not SGI	No	Critical Infrastructure: Critical Infrastructure-Critical Energy Infrastructure Information (18 CFR 388.113), Basic		M	L	L		
Public Technical and non-Technical Information	NUREGs, technical letters, etc.	Yes	N/A	D.20 Knowledge Creation & Management: Research and Development; Knowledge Dissemination	L	L	L	NIST recommends LML, but these are all public, non-proprietary, unauthorized modification does not have an impact on the mission and disruption of access to research and innovation information will have only a limited adverse effect	All
Non-Public Technical Information	Experimental data/files, supporting documents, other research documents not included in final reports, computational codes by staff that are not publicly available,	No	Nuclear: Security-Related Information (NRC RIS 2005-31) Specified	D.20 Knowledge Creation & Management: Research and Development OR D.21	M	M	L	NIST recommends LML, but this the CUI component of this class of information defaults to MML at	All

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
	etc., including CUI that is not SGI							NRC for technical information.	
Hearing Preparation Documents	Pleadings, briefs, motions, hearing files	Yes	N/A	C.2.2 Regulatory Development (all subtypes) and/or D.17.4 Legal Prosecution and Litigation Information Type (Legal prosecution/litigation includes all activities involved with presenting a case in a legal proceeding both in a criminal or civil court of law in an attempt to prove guilt/responsibility)	L	L	L	Consistent with NIST guidance provisional security categorization	NRR, NMSS, NRO, OGC
Hearing Preparation Documents	Pleadings, briefs, motions, hearing files (CUI that is not SGI)	No	Nuclear: Security-Related Information (NRC RIS 2005-31) Specified; Legal: Protective Order (10 CFR 2.1010(b)(6)) Specified		M	M	M	Some hearing documents contain safeguards or other protected information that is discussed elsewhere in this table. In those instances the documents should be protected according to how the information is listed this table (for example, a pleading that contains safeguards information will be treated as a safeguards document as shown in the table.). Many of the CUI hearing documents could be protected as MLL, consistent with how most other types of CUI are treated in the table. However, the MMM level for hearing documents is meant to reflect documents that contain information such as personal privacy, medical, or sensitive security-clearance related information. The MMM level of protection is consistent with the NIST guidance for protecting “personal privacy information.”	NRR, NMSS, NRO, OGC

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
Commission Documents	SECY papers, COMSECYs, SRMs, Voting Records, Correspondence, and Commission Meeting Information, publicly available	Yes	N/A	C.2.8.3 Executive Functions	L	L	L	Based on content of the document or correspondence. There is nothing unique about the fact that information is provided to the Commission.	All
Commission Documents	SECY papers, COMSECYs, SRMs, Voting Records, Correspondence, and Commission Meeting Information, CUI that is not SGI	No	Nuclear: Security-Related Information (NRC RIS 2005-31) Specified	C.2.8.3 Executive Functions	M	L	L		ALL
Commission Procedures	Internal Commission Procedures – during Commission review.	No	N/A	C.2.8.3 Executive Functions	M	L	L	Consistent with NIST guidance provisional security categorization	SECY
Commission Procedures	Internal Commission Procedures - final approved.	Yes	N/A	C.2.8.3 Executive Functions	L	L	L	Consistent with NIST guidance provisional security categorization	SECY
Commission Deliberative Documents	Draft documents, CUI that is not SGI	No	Nuclear: Security-Related Information (NRC RIS 2005-31) Specified		M	L	L	During deliberation, Commission generated documents are treated as CUI.	SECY
Public Interactions	Correspondence (emails, letters)	Yes	N/A	C.2.6 Public Affairs (all subtypes)	L	L	L	Consistent with NIST guidance provisional security categorization	All
International - publicly released information	Correspondence, presentations, MOUs and other agreements with international partners	Yes	N/A	D.5 International Affairs and Commerce (all subtypes)	L	L	L	The NIST guidance provisional security categorization of HHM is overly conservative for publicly available international information.	All
International - non-publicly released information and data sources	Correspondence, presentations, data shared with other agencies that is sensitive, including All CUI that is not SGI	No	International Agreements (10 USC 130c) Specified	D.5 International Affairs and Commerce (all subtypes)	M	M	L	The NIST guidance provisional security categorization of HHM is overly conservative with respect to the NRC mission and international engagement. MML is proposed, particularly for sensitive policy	All

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
								information received from the executive branch or foreign governments.	
Human Resources & Authentication	Information about employee identity, income, or medical conditions used to determine retirement and other benefits	No	Privacy: Personnel (45 USC 362(d)) Basic, (5 CFR 293.106) Specified	C.2.8.9 Personal Identity and Authentication	M	M	M	Consistent with NIST guidance provisional security categorization	All
Human Resources	All other sensitive Workforce Planning and Human Resource Management information	No	Privacy: Personnel (45 USC 362(d)) Basic, (5 CFR 293.106) Specified	C.3.3 Human Resource Management	M	L	L		All
Human Resources	All other Workforce Planning and Human Resource Management information	Yes	N/A	C.3.3 Human Resource Management	L	L	L		All
Accounting and Budget Information - non-publicly available, including CUI that is not SGI	Sensitive accounting information consists of accounting assets, liabilities, fund balances, revenues and expenses associated with the maintenance of Federal funds and expenditure of Federal appropriations (Salaries and Expenses, Operation and Maintenance, Procurement, working Capital, Trust Funds, etc.) that is not publicly released.	No	Financial: Budget (OMB Circular A-11 section 22.1, OMB Memorandum 01-17) Basic	C.3.2.4 Accounting Information and C.2.8.9 Personal Identity and Authentication	M	M	M	Accounting information is LML under NIST standards, however most NRC accounting information contains elements of PII data so it is controlled as MMM.	All
Accounting or Budget Information that is publicly released	Non-sensitive accounting and budgeting information consists of related information that is or has been publicly released under normal business practice.	Yes	N/A	C.3.2.4 Accounting Information	L	L	L	Consistent with NIST guidance.	All
Internal administrative information that does not contain CUI, but	Delegation memos, inventories, non-sensitive schedulers and other transitory records.	No	N/A	C.2.8.12 General Information	L	L	L	Consistent with NIST guidance.	All

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
which is not normally proactively released									
Information Security Policy and Procedures	IT security policies, procedures and controls covering such services as identification, authentication, and non-repudiation considered to be CUI that is not SGI.	No	Information Systems Vulnerability Information (44 USC 3555(f) (previously 44 USC 3545(f))) Basic	C.3.5.5 Information Security	M	M	L	Consistent with NIST guidance.	All
Information Security Policy and Procedures	IT security policies, procedures and controls covering such services as identification, authentication, and non-repudiation not considered to be CUI that is not SGI.	No	N/A	C.3.5.5 Information Security	L	M	L	Consistent with NIST guidance.	All
Information System Vulnerabilities	Information regarding existing information system vulnerabilities	No	Information Systems Vulnerability Information (44 USC 3555(f) (previously 44 USC 3545(f))) Basic	C.3.5.8 System and Network Monitoring Information Type	M[1]	M[2]	L	Consistent with NIST guidance. When the system and network monitoring data being collected supports information types described in this guideline, agency personnel should consider a confidentiality impact assignment of the highest impact information type processed by the system. The integrity impact level recommended for system and network monitoring information associated with highly	

[1] Adjusted to match the highest confidentiality sensitivity level of the information on the system.

[2] Adjusted based upon the information criticality.

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
								critical information is high.	
Budget Execution Information Type	Day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses.	No	Proprietary Business Information: Manufacturer (15 USC 2055(b)) Basic; Privacy: Contract Use (48 CFR 324.102(f)) Basic	C.2.3.5 Budget Execution	M	M	L	The effects of loss of confidentiality of budget execution information can violate privacy regulations, reveal information proprietary to private institutions, and reveal procurement-sensitive information. Public release of sensitive budget execution information can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion.” “In the case of agreements or transactions involving large monetary values, asset losses, and damage to agency operations, the potential for serious loss of public confidence is high. The consequent integrity impact level is moderate to high. If the budget execution information is time-critical or very sensitive, the integrity impact level may be moderate or high.”	
Acquisition Information -	Sensitive acquisition information that has not and	No	Proprietary Business	C.3.4.1 Goods acquisition involves the procurement	M	M	L	The NIST default is LLL, however the	All

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
Procurement-Sensitive, Proprietary, and other CUI information that is not SGI	will not be made publicly available.		Information: Manufacturer (15 USC 2055(b)) Basic; Privacy: Contract Use (48 CFR 324.102(f)) Basic	of physical goods, products, and capital assets to be used by the Federal government				standard acknowledges that Proprietary information is MML under the CUI guidance.	
Acquisition Information - publicly available and publicly released.	Much of the acquisition information obtained by or used by the NRC is publicly available, and we proactively release a large amount of acquisition information that is otherwise not available. This applies to any acquisition information that is not Proprietary or otherwise CUI that is not SGI, when that information is not being controlled as procurement-sensitive.	Yes	N/A	C.3.4.1 Goods acquisition involves the procurement of physical goods, products, and capital assets to be used by the Federal government	L	L	L	Consistent with NIST guidance provisional security categorization	All
SGI Information	All document types that have SGI marking which includes: rulemaking and guidance documents, licensing documents, enforcement documents, etc.	No	Nuclear: Safeguards Information (10 CFR Part 73) Specified	C.3.1.1 Facilities, Fleet, and Equipment Management Information Type; D.7.1 Energy Supply Information Type	H	M	L	Consistent with NIST guidance provisional security categorization recognizing the special significance of safeguards information as defined in the Atomic Energy Act, as amended.	All
Licensing information provided to Law Enforcement for Border and Transportation Security	This special type of information covers the information made available specifically for use by Border Protection and Law Enforcement Agencies. The same information may be LLL in other applications.	No	Nuclear: Security-Related Information (NRC RIS 2005-31) Specified	D.2.1 Border and Transportation Security Information	M	M	M	Consistent with NIST guidance provisional security categorization	NMSS, OIP, NSIR
Incident Response Information	Incident response information, including computer codes, designated specifically for use in NRC's PMEF functions	No	Nuclear: Security-Related Information (NRC RIS 2005-31) Specified	D.4.1 Disaster Monitoring and Prediction Information and C.2.4.2 Continuity of Operations Information	M	H	H	Consistent with NIST guidance provisional security categorization	RES, NMSS, NSIR, NRR, NRO

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
	considered to be CUI that is not SGI.								
Incident Response Information	Information, including computer codes, designated specifically for use in NRC's PMEF functions. The same information may be LLL in other applications.	No	Nuclear: Security-Related Information (NRC RIS 2005-26) Basic	D.4.1 Disaster Monitoring and Prediction Information and C.2.4.2 Continuity of Operations Information	L	H	H	Consistent with NIST guidance provisional security categorization	RES, NMSS, NSIR, NRR, NRO
Personal Identity and Authentication Information and Security Management Information Type (this item to be further refined)	ACCESS uses this information type in the PIV card lifecycle component. During the PIV card lifecycle, the system captures the applicant's name, social security number, clearance information, date of birth, fingerprints, telephone number, home address, work e-mail address, and Local Area Network (LAN) account information. The aforementioned information is stored in the Authentication and Credentialing Services (ACS) SQL server, which is outside the system boundary of ACCESS. ACCESS workstations used in the PIV lifecycle access this personal data via the ACS web server. The PIV card, contains sensitive information including the cardholder unique identifier (CHUID), PIV PIN (8 digits), two biometric fingerprints, and authentication data including the PIV authentication key, card authentication key, digital signature key, and key management key. All keys are generated and maintained on the card except for the key management key, which is escrowed to ensure that user	No	Information Systems Vulnerability Information (44 USC 3555(f) (previously 44 USC 3545(f))) Basic	C.2.8.9 Personal Identity and Authentication Information Type Personal identity and authentication information includes that information necessary to ensure that All persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. This information include individual citizen's Social Security Numbers, names, dates of birth, places of birth, parents' names, etc.	H	H	M	NIST recommended security categorization for the personal identity and authentication information type is as follows: Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}. Since the Personal Identity and Authentication Information processed by ACCESS is used in controlling access to federal facilities, the severe consequences of unauthorized disclosure that permits forgery of credentials justifies a High impact assignment to Confidentiality and Integrity. Since information associated with security management processed by ACCESS can be of material use to personnel seeking to penetrate and/or commandeer NRC facilities, NRC	ADM, OCIO

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
	encrypted data can be retrieved in an emergency. The ACCESS physical access control system (PACS) contains sensitive information including the CHUID, PACS PIN (four digits), applicant's name, clearance information, and assigned access rights.							information, or NRC information systems, a High impact to Confidentiality is justified. Since the consequences of authorized modification or destruction of time-critical security management information can reasonably be expected to result in physical security vulnerabilities, a High impact to integrity is justified. Since the unauthorized modification or destruction of the security management information processed by ACCESS, to include alarm and alert communications and interconnections for security management systems and automated control systems that support security management processes, can have a serious adverse effect on agency operations, agency assets, or individuals, a Moderate impact assignment to Availability is justified	
Adjudicatory Documents	Pleadings, briefs, motions, orders, decisions, etc.	Yes	N/A	D.17.1 Judicial Hearings Information Type	L	L	L	Any information that is public in nature requires no additional protection. This deviates from the recommended impact level of moderate. Since there are no	Commission, SECY, and ASLBP

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
								consequences if publically available is disclosed and impact level of Low for confidentiality is appropriate. This level of confidentiality is also appropriate even if PII is filed in an adjudicatory proceeding. The NRC privacy policy states "Any comments submitted to the NRC will generally be made public, including any personally identifiable information included in a submission. Unless excluded pursuant to an order of the Commission, an Atomic Safety and Licensing Board, or a Presiding Officer, documents submitted in adjudicatory proceedings will appear in NRC's Electronic Hearing Docket that is available to the public. Therefore, hearing participants should not include personal privacy information, such as social security numbers and dates of birth, in their filings."	
Adjudicatory Documents	Pleadings, briefs, motions, orders, decisions, etc.	No	Proprietary Business Information:	D.17.1 Judicial Hearings Information Type	M	L[3]	L	Information that rises to the level of sensitive unclassified non-	Commission, SECY, and ASLBP

[3] NIST recommends "Low" as the provisional integrity impact level. However, the Judicial Hearings Information Type integrity impact level is commensurate with integrity impact level of the originating source of the information.

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
			Manufacturer (15 USC 2055(b)) Basic; Privacy: Personnel (45 USC 362(d)) Basic, (5 CFR 293.106) Specified; Legal: Protective Order (10 CFR 2.1010(b)(6)) Specified					safeguards material should be treated with moderate confidentiality. This information includes categories such as business proprietary or PII when excluded by a Licensing Board.	
Adjudicatory Documents	Pleadings, briefs, motions, orders, decisions, etc.	No	Proprietary Business Information: Manufacturer (15 USC 2055(b)) Basic; Privacy: Personnel (45 USC 362(d)) Basic, (5 CFR 293.106) Specified; Legal: Protective Order (10 CFR 2.1010(b)(6)) Specified	D.17.1 Judicial Hearings Information Type	H	L[4]	L	Any information above sensitive unclassified non-safeguards material	Commission, SECY, and ASLBP
Criminal History Records Information	Related to information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release.	No	Law Enforcement: Criminal History Records Information (28 CFR 20) Specified		H	M	L	Consistent with CUI law reference	NRO, NRR

[4] Ibid

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.	N	Critical Infrastructure, Basic		M	M	M	Consistent with CUI law reference	
Critical Infrastructure/ Physical Security	Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.	N	Critical Infrastructure: Physical Security, Specified GSA PBS P 3490.2		M	M	M	Consistent with CUI law reference	
Critical Infrastructure/ Protected Critical Infrastructure Information	As defined by 6 USC 131-134, and 6 CFR 29, PCII relates to threats, vulnerabilities, or operational experience related to the national infrastructure. PCII offers protection to private sector infrastructure information voluntarily shared with government entities for purposes of homeland security.	N	Critical Infrastructure: Protected Critical Infrastructure Information, Specified 6 CFR 29		M	M	M	Consistent with CUI law reference	
Emergency Management	Related to information concerning the continuity of executive branch operations during all-hazards emergencies or other situations that may disrupt normal operations.	N	Emergency Management, Basic		M	M	M	Consistent with CUI law reference	

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
Financial/ Electronic Funds Transfer	Relating to the computer-based systems used to perform financial transactions electronically.	N	Financial: Electronic Funds Transfer, Basic		M	M	L	Consistent with CUI law reference	OCFO
Financial/ Retirement	Related to post-employment funding provided by an employer.	N	Financial: Retirement, Basic		M	M	L	Consistent with CUI law reference	OCHCO
Law Enforcement/ Communication s	Related to the contents of any wire, oral, or electronic communication.	N	Law Enforcement: Communication, Basic		M	M	M	Consistent with CUI law reference	NSIR
Law Enforcement/ Investigation	Related to information obtained during the course of a law enforcement investigation.	N	Law Enforcement: Investigation, Specified 18 CFR 1b.20, 21 CFR 20.64(d)(4)		H	H	M	Consistent with CUI law reference	OI, OIG
Law Enforcement/ Whistleblower Identity	Identity of any individual, or 2 or more individuals acting jointly, who provides information relating to a legal violation or illicit activity, including information provided by a whistleblower which could reasonably be expected to reveal the identity of a whistleblower.	N	Law Enforcement: Whistleblower Identity, Basic		M	M	L	Consistent with CUI law reference	OI, OIG
Legal/ Administrative Proceedings	Adjudication of agency-related matters including, but not limited to, dispute resolution, settlements, and issuances of orders	N	Legal: Administrative Proceedings, Specified 16 CFR 3.45, 17 CFR 10.64		M	M	L	Consistent with CUI law reference	
Legal/ Collective Bargaining	Defining agencies' and representatives' duty to negotiate in good faith to include disclosure of certain labor relations training and guidance materials and limiting the	N	Legal: Collective Bargaining, Basic		M	M	L	Consistent with CUI law reference	

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
	issuance of certain subpoenas.								
Legal/Privilege	Per 12 USC 78x: The term "privilege" includes any work-product privilege, attorney-client privilege, governmental privilege, or other privilege recognized under Federal, State, or foreign law. Per 502(g): (1) "attorney-client privilege" means the protection that applicable law provides for confidential attorney-client communications; and (2) "work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial.	N	Legal: Privilege, Basic		M	M	L	Consistent with CUI law reference	OGC
Nuclear	Related to protection of information concerning nuclear reactors, materials, or security.	N	Nuclear, Specified 42 USC 2077(a)		M	M	L	Consistent with CUI law reference	
Nuclear/ Naval Nuclear Propulsion Information	Related to the safety of reactors and associated naval nuclear propulsion plants, and control of radiation and radioactivity associated with naval nuclear propulsion activities, including prescribing and enforcing standards and regulations for these areas as they affect the environment and the safety and health of workers, operators, and the general public. Specified 50 USC 2511	N	Nuclear: Naval Nuclear Propulsion Information, Specified 50 USC 2511		H	H	L	Consistent with CUI law reference	
Nuclear/ Unclassified Controlled	Relating to certain design and security information concerning nuclear facilities,	N	Nuclear: Unclassified Controlled		H	H	L	Consistent with CUI law reference	

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
Nuclear Information - Energy	materials, and weapons, specific to the Department of Energy.		Nuclear Information – Energy, Specified 10 CFR 1017						
Privacy	Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-07-16, or "means of identification" as defined in 18 USC 1028(d)(7).	N	Privacy, Specified OMB M-07-16		M	M	L	Consistent with CUI law reference	
Privacy/Death Records	Related to information contained within an official document issued by a public registry verifying that a person has died, with information such as the date and time of death, the cause of death, and the signature of the attending or examining physician.	N	Privacy: Death Records, Basic		M	M	L	Consistent with CUI law reference	
Privacy/Health Information	As per 42 USC 1320d(4), "health information" means any information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.	N	Privacy: Health Information, Specified 18 USC 3486(e), 42 USC 1320d-2(d)(2), 20 CFR 401.200(g), 29 CFR 1630.14(b)(1), 42 CFR 2.16(a)		M	M	L	Consistent with CUI law reference	
Privacy/ Inspector General	Related to the identity of a person making a report to the Inspector General of any Executive agency.	N	Privacy: Inspector General,		M	M	L	Consistent with CUI law reference	OIG

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
			Specified 5 USC Appendix 8D(e)						
Privacy/Military	Any member or former member of the armed forces or affiliated organization of the Department of Defense.	N	Privacy: Military, Basic		M	M	L	Consistent with CUI law reference	
Procurement and Acquisition	Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.	N	Procurement and Acquisition, Specified 48 CFR 3.104-4, 48 CFR 52.215-1(e)		M	M	L	Consistent with CUI law reference	
Procurement and Acquisition/ Small Business Research and Technology	Relating to certain "Small Business Innovation Research Program" and "Small Business Technology Transfer Program" information in a government database, as referenced in 15 USC 638(k)(2).	N	Procurement and Acquisition: Small Business Research and Technology, Basic		M	M	L	Consistent with CUI law reference	
Procurement and Acquisition/ Source Selection	Per FAR 2.101: any of the following information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly: (Items 1-10).	N	Procurement and Acquisition: Source Selection, Specified 48 CFR 14.303, 48 CFR 14.402-1(a), 48 CFR 15.609(a), 48 CFR 14.401(a), 48 CFR 3.104-4, 48 CFR 52.215-1(e)		M	M	L	Consistent with CUI law reference	
Proprietary Business Information	Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and	N	Proprietary Business Information, Specified 15 USC 2055(a), 21 USC 331(j), 21 USC 355(c)(3)(D)(i)(III		M	M	L	Consistent with CUI law reference	

NRC Information Type	Information Description	Public Avail? Y/N	Applicable CUI References	Applicable NIST Information Type (from NIST SP 800-60)	Conf H/M/L	Integ H/M/L	Avail H/M/L	Rationale for Selected Sensitivity Level as H/M/L	Office(s)
	development; existing and future product designs and performance specifications.		), 33 USC 1322(g)(3), 51 USC 20131(b), 28 CFR 100.20, 40 CFR 2.205(c), 48 CFR 225.7304(c), 48 CFR 52.203-13, 10 USC 2320(a)(2)(B), 17 CFR 140.98, 15 USC 3710a(c)(7), 42 USC 1306(f), 19 USC 1332(g), 19 USC 2436(a)(4), 19 USC 2252(a)(8), 19 USC 2252(i), 19 USC 1337(n), 19 USC 1677f(b), 19 USC 1677f(c), 19 USC 1677f(f), 19 CFR 201.6, 19 CFR 206.7, 19 CFR 206.8, 19 CFR 206.17, 19 CFR 206.54(e), 19 CFR 210.5(b), 19 CFR 210.5(d), 19 CFR 210.5(e), 19 CFR 210.34(c)(1), 19 CFR 210.72, 19 CFR 207.3, 19 CFR 207.4, 19 CFR 207.7, 19 CFR 207.51, 19 CFR 207.93						

OCIO-CS-PROS-2001 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
08-Mar-17	1.1	Added types specified by CUI that NRC uses	Computer security process web page	As needed
10-Jan-17	1.0	Initial Release	Computer security process web page	As needed