Nuclear Regulatory Commission
Computer Security Office
Computer Security Process

Office Instruction:	CSO-PROS-1325
Office Instruction Title:	Authority to Use Process
Revision Number:	1.0
Effective Date:	February 15, 2014
Primary Contacts:	Kathy Lyons-Burke, SITSO
Responsible Organization:	CSO/PCT
Summary of Changes:	CSO-PROS-1325, "Authority to Use Process" defines the process that must be followed to obtain an Authority to Use a system owned by another agency that is not customized for NRC.
Training:	As needed
ADAMS Accession No.:	ML13330B640

Concurrences			
Primary Office Owner	Policy, Standards, and Training		
Responsible SITSO	Kathy Lyons-Burke		**Date of Concurrence**
Directors	CSO	Tom Rich**/RA/**	19-Dec-13
	PCT	Kathy Lyons-Burke**/RA/**	19-Dec-13
	CSA	Thorne Graham**/RA/**	19-Dec-13

Concurrence Meeting Conducted on 19-Dec-13			
Attendees:	Tom Rich	Kathy Lyons-Burke	Jonathan Feibus

Table of Contents

Computer Security Process
CSO-PROS-1325

Authority to Use Process

---

1 PURPOSE

CSO-PROS-1325, Authority to Use Process, defines the process that must be followed to obtain an Authority to Use a system that has a Federal Information Security Management Act (FISMA) Authority to Operate (ATO) issued by another agency where that system will contain NRC data, but is not customized for NRC (customization requires an NRC issued ATO). Customization includes input, output, or processing that is customized for NRC and does not refer to customized reporting. This type of system will be referred to as a "sponsor agency system."

Interconnecting systems can expose the participating organizations to risk. If the interconnection is not properly designed, configured, and secured, security failures could compromise the connected systems and the data that they store, process, or transmit. Similarly, if one of the connected systems is compromised, the interconnection could be used as a conduit to compromise the other system and its data. The potential for compromise is underscored by the fact that, in most cases, the participating organizations have little or no control over the operation and management of the other party's system nor do they have visibility into the security of the system. The purpose of this process is to minimize the risk of using systems operated by another agency.

An authority to operate a system is granted by an agency that has responsibility for the operation and maintenance of that system. Once a system has obtained an authority to operate from that agency, the system can operate as long as that authority remains intact. In order for NRC to use that system, NRC must authorize use of the sponsor agency system.

The information in this document is intended to be used by System Owners (SO), Information System Security Officers (ISSO), System Administrators (SA), Assessment Project Managers, and Assessors.

2 GENERAL REQUIREMENTS

When an NRC organization chooses to use a system that is authorized to operate by another agency, the NRC organization must obtain an Authority to Use (ATU) that system from the NRC Designated Approving Authority (DAA). If the authorization issued by the sponsor agency is not current, NRC will not grant an ATU. Note that an ATU is not required for access (via the public internet) to sponsor agency systems where no NRC data is stored or processed.

All documents required by this process must be placed into the Agencywide Documents Access and Management System (ADAMS) and the accession number supplied in the ATU request (see CSO-TEMP-1325).

2.1 Definitions

Assessment Project Manager — The individual responsible for developing and distributing the Project Plan for a system assessment, monitoring to ensure actions occur in accordance with the plan, and for revising the plan if necessary during the course of the assessment. The Assessment Project Manager serves as the primary contact for issues that may impact or delay key assessment activities.

Assessor — The individual(s) conducting security control testing, configuration checks, and vulnerability scans.

Sponsor Agency — Federal agency responsible for authorizing operation of and operating and maintaining the system that NRC wishes to use

2.2 References

- Federal Information Processing Standards and National Institute of Standards and Technology (NIST) publications can be found at: http://csrc.nist.gov/.
- NIST Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, as revised
- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, as revised
- NRC CSO documents can be found at http://www.internal.nrc.gov/CSO/.
- Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems
- Federal Information Processing Standard (FIPS) Publication 140-2, Security Requirements For Cryptographic Modules
- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, as amended
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, as amended
- NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, as amended
- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, as amended
- CSO-PROS-2030, “NRC Risk Management Framework (RMF) and Authorization Process,”
- CSO-STD-0020, “Organization Defined Values for System Security Controls”
- CSO Web Page (http://www.internal.nrc.gov/CSO/) for policies, standards, processes, procedures, templates and guidance other than those specifically listed

3 INITIAL SYSTEM USE ANALYSIS

The initial system use analysis identifies the data types to be used in the sponsor agency system and the security categorization of the sponsor agency system. The purpose of the analysis is to ensure that the sponsor agency system is at a sensitivity level at or above that of

the NRC information types to be used with the system and that any information types from the sponsor agency system to be used with an NRC system are at or below the sensitivity level of the NRC system. The NRC system owner must ensure that an initial system use analysis is performed before seeking an ATU for the sponsor agency system.

The Security Categorization that was performed for an NRC system that includes the data types that will be used with the sponsor agency system is used to identify the data types. The security categorization is identified along with the specific data types and their sensitivity level.

The NRC information security categorization for confidentiality, integrity, and availability levels must be compared against the sponsor agency's system security categorization for confidentiality, integrity, and availability levels to ensure that the NRC values are at or below those specified in the system's approved security categorization document.

The information types from the sponsor agency system that will be used with the NRC system must also be categorized. The NRC information security categorization for confidentiality, integrity, and availability levels of information types from the sponsor agency system must be compared against the NRC system security categorization for confidentiality, integrity, and availability levels of the NRC system to ensure that the sensitivity levels are at or below those specified in the NRC system's approved security categorization document.

If there is a mismatch between the sensitivity levels, the NRC cannot use the sponsor agency's system. CSO must approve the security categorization before the ATU package is submitted. Documentation of this comparison must be provided as part of the ATU request package.

4 SYSTEM INTERCONNECTION

Interconnections are used to communicate with the sponsor agency system. If the only interconnection is via a standard web interface, the method of use of the sponsor agency system must be documented as part of the ATU request package.

4.1 System Interconnection Types

The system owner must ensure that the type of interconnection to the NRC is identified in the ATU request package. The various interconnection types include:

4.1.1 NRC-to-Sponsor-Agency-System Over Private Circuit

An NRC-to-Sponsor-Agency-System over private circuit connection is defined as a connection from an NRC system to the sponsor agency system that uses a private communications channel owned by NRC or the sponsor agency or leased from a common carrier, such as Verizon or AT&T.

4.1.2 NRC-to-Sponsor-Agency-System Over Internet

An NRC-to-Sponsor-Agency-System over the Internet connection is defined as a connection from an NRC system to the sponsor agency system that traverses the Internet. This type of connection includes use of a sponsor agency's web-based system.

4.2 Interconnection Documentation

All system interconnections must be documented. If system access is achieved through a standard web interface on the Internet, this must be documented in the ATU request along with the cryptographic modules that are used to protect sensitive NRC information. Please note that all cryptographic modules must be NIST FIPS 140 validated and operated in FIPS mode. All interconnection agreements between NRC and another organization must be signed by the NRC Chief Information Officer (CIO).

4.2.1 Interconnection Security Agreement

An Interconnection Security Agreement (ISA) is a security document that specifies the technical and security requirements for establishing, operating, and maintaining an interconnection for the purposes of data exchange. The intent of the ISA is to document and formalize the interconnection arrangements between the NRC and another organization to specify any details that may be required to provide overall security safeguards for the systems being interconnected. An ISA may be tailored by mutual consent of the participating organizations. A system that is approved by an ATU for interconnection must meet the protection requirements equal to, or greater than, those implemented by the NRC. For instance, if a high-impact security control baseline is required for the NRC system, in most cases, a high-impact security control baseline will be required for the connecting system.

The ISA must be documented using the CSO-TEMP-2010, Interconnection Security Agreement (ISA) template.

5 REQUIRED DOCUMENTATION

The documentation for any NRC systems involved in the interconnection with the sponsor agency system must be updated.

5.1 NRC System Security Plan

The System Security Plan (SSP) is the primary document for describing the security of an NRC system. All system interconnections other than standard web Internet connections must be documented in the System Interconnections/Information Sharing section of the SSP of the interconnected NRC system, regardless of the type or purpose of the system interconnection. The description must include an overview of the interconnection, and a summary of the interconnection agreement. The System Description section of the SSP must document all interconnection details. Additionally, there may be several security controls that are directly impacted by an interconnection (e.g., CA-3 Information System Connections) and implementation details for these controls must be provided accordingly. In addition, any interconnection-related hardware and software must be included in the system's inventory.

The current NRC SSP of the system to be interconnected must include:

- Names of the interconnected systems;
- Names of the sponsor agency organizations responsible for the sponsor agency system;
- FIPS 199 category of the sponsor agency systems;
- ATO status of the sponsor agency system (including ATO expiration date);
- Type of interconnection;
- Interconnection documentation type (e.g. MOU/ISA, ATU, SLA);
- Date of agreement;

- Name and title of management official(s) that authorized the sponsor agency system to operate

5.2 NRC System PIA

The Privacy Impact Assessment (PIA) for any NRC system connecting with the sponsor agency system must be updated if there are new information types resulting from the interconnection.

5.3 NRC System Security Categorization

The security categorization for any NRC system connecting with the sponsor agency system must be updated if there are new information types resulting from the interconnection.

5.4 Memorandum of Understanding

The Memorandum of Understanding (MOU) documents the terms and conditions for sharing data and information resources in a secure manner. Specifically, the MOU:

- Defines the purpose of the interconnection;
- Identifies relevant authorities;
- Specifies the responsibilities of both organizations; and
- Defines the terms of agreement, including the apportionment of costs and the timeline for terminating or reauthorizing the interconnection.
- Is used to document the business and legal requirements necessary to support the business relations between the two organizations and should not include the technical details on how the interconnection is established or maintained; that is the function of the ISA (see section 4.2.1).

All MOUs between NRC and another organization must be signed by the NRC CIO.

5.4.1 NRC Service Level Agreement

Service Level Agreements (SLA) define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance[1].

Whenever an NRC system inherits interconnection-related security services from another system, these services must be detailed in an SLA. The SLA documents the expected services and the level of confidentiality, integrity, and availability provided. An SLA is typically used to document an interconnection where one system is dependent on the other, but not vice versa.

All SLAs between NRC and another organization must be signed by the NRC CIO.

5.4.2 ISSO Appointment Letter for NRC ISSO of Sponsor Agency System

An NRC ISSO (primary and alternate) must be appointed to oversee the day-to-day security requirements for sponsor agency systems and serves as the NRC point of contact for cyber security issues related to the sponsor agency system. This individual must have an

[1] Reference: NIST SP800-53 (Revision 3), control SA-9.

understanding of the information that is being shared between the NRC and the sponsor agency. The system owner appoints the NRC ISSO for the sponsor agency system using CSO-TEMP-0001, "System Information System Security Officer (ISSO) Appointment."

The ISSO must have detailed knowledge and expertise required to manage the security aspects of the system and the information. In this context, an NRC ISSO must be assigned to ensure:

1. Day-to-day security operations of the interconnected system(s) are carried out;
2. Terms of MOU/ISA or ATU are carried out;
3. NRC data is always adequately protected as commensurate with its sensitivity; and
4. All risks are identified and communicated to the NRC System Owner.

Additionally, the NRC ISSO will be the primary liaison between the NRC and the point-of-contact (POC) of the interconnected system during the interconnection approval process. Also, the NRC ISSO is responsible for meeting all annual cyber security requirements for the system.

5.5 NRC System ISSO Appointment Letter

The ISSO appointment letter for any NRC systems involved in the interconnection with the sponsor agency system must be provided as part of the ATU request. This letter is generated using the CSO-TEMP-0001, System Information System Security Officer (ISSO) Appointment Letter template.

5.6 Contingency Plan Test Verification

The ATU request must contain verification that the sponsor agency system has performed annual contingency plan testing. A memorandum from the agency that owns or operates the system or an email from the sponsor agency system owner must be provided with the ATU request that confirms completion of annual CP testing, including date test was completed.

5.7 Annual Control Testing Verification

The ATU request must contain verification that the sponsor agency system has performed annual security control testing. A memorandum from the agency that owns or operates the system or an email from the sponsor agency system owner must be provided with the ATU request that confirms completion of annual control testing, including date test was completed.

5.8 Sponsor Agency System Contact Information

The ATU request must identify the sponsor agency system Point-of-Contact (POC) and contact information for the following:

- Sponsor agency system owner
- Sponsor agency system ISSO

5.9 Sponsoring Agency ATO Memo

The ATO memo issued for the sponsor agency system by the sponsor agency system must be provided as part of the ATU, along with the expiration date of the current ATO, the agency's certification/security control assessment, and confirmation of the completion of annual Federal Information Security Management Act (FISMA) requirements.

6 ATU REQUEST MEMO

The ATU request memo is prepared using CSO-TEMP-1325.

7 ATU PACKAGE REVIEW

The NRC DAA provides the ATU package to the Chief Information Security Officer (CISO) and requests an authorization recommendation from the CISO. The CISO uses Computer Security Office (CSO) resources to review the ATU package. In many cases, the CSO will contact the sponsor agency system POC to obtain access to system information for review. Once the review is completed, the CISO provides a recommendation to the NRC DAA.

8 ATU DECISION

The NRC DAA reviews the ATU package and the CISO authorization recommendation and makes a risk-based decision whether or not to issue an ATU for the system.

9 ANNUAL REQUIREMENTS FOR SYSTEMS GRANTED AN ATU

Once a system is granted an ATU by the NRC DAA, the system owner is responsible for meeting all annual reporting requirements. The system owner must notify the DAA for Major Information Technology (IT) Investments of a sponsor agency system ATO expiration or termination, significant changes, unacceptable risks or any changes to the MOU / ISA at least 30 calendar days in advance of such events.

The following must be provided to CSO annually on or before the date of the last documentation of that type:

1. Verification that day-to-day security operations of the interconnected system(s) are carried out including periodic vulnerability assessment scanning, annual CP testing and annual control testing.
2. Evidence of the execution of annual contingency plan testing and annual security control testing *within one year and one month of the previous test report date*.
3. Assurance that terms of any applicable Memorandum of Understanding (MOU), Interconnection Security Agreement (ISA), and Authority to Use (ATU) are reviewed annually and are carried out accordingly[2].
4. Assurance that the sponsoring agency maintains the system ATO in accordance with NIST Special Publication (SP) 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems.
5. Assurance that the system maintains its authorization granted by the NRC Designated Approving Authority (DAA), and is re-authorized by the NRC DAA upon any significant change that might give rise to additional/other risks.
6. Verification of the currency of the sponsor agency ATO for the sponsor agency system

---

2 Enter the most recent MOU and ISA in ADAMS as an OAR and submit to CSO by emailing the ADAMS ML# to RidsCsoMailCenter Resource by September 15, 2014.

10 ACRONYMS

ADAMS	Agencywide Documents Access and Management System
ATO	Authority to Operate
ATU	Authority to Use
CISO	Chief Information Security Officer
CSO	Computer Security Office
DAA	Designated Approving Authority
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
ISA	Interconnection Security Agreement
ISSO	Information System Security Officer
NIST	National Institute for Standards and Technology
OIS	Office of Information Services
POC	Point of Contact
PIA	Privacy Impact Assessment
RMF	Risk Management Framework
SITSO	Senior Information Technology Security Officer
SA	System Administrators
SLA	Service Level Agreement
SO	System Owners
SP	Special Publication
SSP	System Security Plan

CSO-PROS-1325 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
29-Jan-14	1.0	Initial issuance	CSO web page and email distribution to ISSOs	As needed