

Nuclear Regulatory Commission Computer Security Office Computer Security Template

Office Instruction: CSO-TEMP-2019

Office Instruction Title: System Authorization Package Transmittal Memo for Sensitive Unclassified Non-Safeguards Information (SUNSI) Systems

Revision Number: 2.0

Effective Date: July 10, 2014

Primary Contacts: Kathy Lyons-Burke, SITSO

Responsible Organization: CSO/PCT

Summary of Changes: CSO-TEMP-2019, "System Authorization Package Transmittal Memo for SUNSI Systems" provides the template that must be used to submit a system authorization package to the NRC Designated Approving Authority (DAA) and request an authority to operate for a sensitive unclassified non-Safeguards information NRC system.

Training: Upon Request

ADAMS Accession No.: ML14120A253

Concurrences			
Primary Office Owner	Policy, Standards, and Training		
Responsible SITSO	Kathy Lyons-Burke		Date of Concurrence
Directors	CSO	Thomas Rich	12-Jun-14
Other Stakeholders	PCT	Kathy Lyons-Burke	12-Jun-14
	CSA	Thorne Graham	12-Jun-14

Concurrence Meeting Conducted on 12-Jun-14			
Attendees:	Thomas Rich	Kathy Lyons-Burke	Thorne Graham

Computer Security Template CSO-TEMP-2019

System Authorization Package Transmittal Memo

1 PURPOSE

The purpose of CSO-TEMP-2019, "System Authorization Package Transmittal Memo" is to submit a system authorization package to the NRC DAA and request an authority to operate a Sensitive Unclassified Non-Safeguards Information (SUNSI) system. System authorization packages and DAA approval are required by the Federal Information Security Management Act (FISMA) and Management Directive and Handbook 12.5, NRC Cyber Security Program.

This front matter and all explanatory information up through the change history table apply to the template only. The front matter and explanatory information must be removed before completing and submitting the memo.

2 TEMPLATE INSTRUCTIONS

The template sections are completed by the system owner organization. Information in <blue> in the template should be replaced with the required information and the font color returned to black before submitting the authorization form.

The date of the memorandum is provided where <Memo Date> is shown and formatted as "Month Day, Year"

The NRC system owner's first name, middle initial, and last name are provided where <System Owner Firstname X. Lastname> is shown.

The NRC system owner's office, region, or Office of Information Services division name is provided where <Office or Region Name> is shown.

The name of the system is provided where <System Name> is shown.

The system acronym is placed wherever <System Acronym> occurs.

The formal request for an authority to operate must be for the specific boundary assessed. This can be for a full system or for a subsystem. If the authorization request is for a subsystem, the subsystem name is provided where <Subsystem Name> is shown and the subsystem acronym is provided where <Subsystem Acronym> is shown. So, for an authorization request for a full system, the sentence would read:

This memorandum constitutes my formal request for an authority to operate for the Azzz Bzzz Czzz (ABC) system.

And for an authorization request for a subsystem, the sentence would read:

This memorandum constitutes my formal request for an authority to operate for the Xaa Yaa Zaa (XYZ) subsystem of the Azzz Bzzz Czzz (ABC) system.

The first name, middle initial, and last name of the individual who will be the primary contact for all matters related to the system security authorization are provided where <Contact First name X. Last name> is shown.

The telephone number of the primary contact is provided where <XXX-XXX-XXXX> is shown.

The overall security categorization (low, moderate, or high) of the system is provided where <system security categorization level> is shown. The breakout immediately following this value indicates the specific level for confidentiality, integrity, and availability breakout that are used to determine the overall value. The level for each is provided where [low, moderate, high] is shown.

The security documentation table identifies required documentation that must be provided as part of an authorization request. Additional documents may be determined to be relevant and can be added to the table. The table below identifies mandatory and optional documentation. The Agencywide Document Access and Management System (ADAMS) accession number for each required document is provided where <Accession Number> is shown.

Document Title	Document Requirement
Business Impact Analysis	Required
Contingency Plan	Required
Deviation Request Memorandum	Required if deviations are being requested
Deviation Request Spreadsheet	Required if deviations are being requested
Information System Security Officer Appointment Letter	Required
Interconnection Security Agreement for Interfacing Systems	Mandatory for interfaces with external systems; Recommended for interfaces with internal systems
Memorandum of Understanding for Interfacing Systems	Mandatory for interfaces with external systems; Recommended for interfaces with internal systems
Plan of Actions and Milestones	Required
Privacy Threshold Analysis (PTA)	Required
Privacy Impact Assessment (PIA)	Required unless a PTA determined a PIA was unnecessary
Security Categorization	Required
Security Risk Assessment	Required
Service Level Agreement between systems	Mandatory for services provided by/for external systems; Recommended for services provided by/for internal systems

Document Title	Document Requirement
System Security Assessment Plan	Required
System Security Assessment Report	Required
System Security Plan	Required
Vulnerability Assessment Report	Required

The Business Impact Analysis (BIA) must be prepared in accordance with CSO-TEMP-2022, Business Impact Analysis Report.

The Contingency Plan (CP) must be prepared in accordance with CSO-TEMP-2023, Contingency Plan.

If there are deviation requests for one or more controls, the Deviation Request Memorandum must be prepared in accordance with CSO-TEMP-2017, Formal Deviation Request Memo, and the Deviation Request Spreadsheet must be prepared in accordance with CSO-TEMP-2018, Deviation/Waiver Request Memo Enclosure. Otherwise, these rows are deleted from the table.

The Information System Security Officer Appointment Letter must be prepared in accordance with CSO-TEMP-0001, System Information System Security Officer (ISSO) Appointment Letter.

If an Interconnection Security Agreement (ISA) has not been developed and is not required, this row should be deleted from the table. If one or more ISAs are required or have been developed, the ISAs for Interfacing Systems must be prepared in accordance with CSO-TEMP-2010, Interconnection Security Agreement (ISA). There must be one row per ISA.

If a Memorandum of Understanding (MOU) has not been developed and is not required, this row should be deleted from the table. If one or more MOUs are required or have been developed, the MOUs for Interfacing Systems must be prepared in accordance with CSO-TEMP-2008, Memorandum of Understanding (MOU) for Interfacing Systems. There must be one row per MOU.

The Plan of Actions and Milestones must be prepared in accordance with CSO-PROS-2016 U.S. Nuclear Regulatory Commission Plan of Action and Milestones Process.

Either a Privacy Threshold Analysis (PTA) or a Privacy Impact Assessment (PIA) PTA must be provided. A PTA is sometimes performed first to determine if a PIA is required. If the PTA determination is that a PIA is not required, the system owner can provide a PTA using the PTA template (ML091970114). Otherwise, a PIA must be provided in accordance with the PIA Manual August 2011 (ML11143A050), PIA Procedures (ML040700596), and the PIA template (ML050460335).

The Security Categorization must be prepared in accordance with CSO-TEMP-2001, System Security Categorization Report and approved by the CSO Policy, Compliance, and Training Senior IT Security Officer.

The Security Risk Assessment (SRA) must be prepared by the DAA-approved independent assessor that assessed the system.

If a Service Level Agreement (SLA) has not been developed and is not required, this row should be deleted from the table. If one or more SLAs are required or have been developed, the SLAs for Interfacing Systems must be prepared in accordance with CSO-TEMP-2009, Service Level Agreement (SLA). There must be one row per SLA.

The System Security Assessment Plan and Report must be developed by a DAA-approved independent assessor.

The System Security Plan (SSP) must be prepared in accordance with the security categorization and with CSO-TEMP-2005, CSO-TEMP-2006, or CSO-TEMP-2007.

The Vulnerability Assessment Report (VAR) must be developed by a DAA-approved independent assessor.

The first name, middle initial, and last name of the primary assessor for the system are provided where [<Security control assessor>](#) is shown.

The security control assessor is required to assess all system controls. The total number of system controls required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations for the system is provided where [<controls assessed>](#) is shown.

The number of controls that are fully in place is provided where [<in place controls>](#) is shown.

The number of controls that are only partially in place is provided where [<partial controls>](#) is shown.

The number of controls that are planned is provided where [<planned controls>](#) is shown.

The number of controls that are not applicable to the system is provided where [<NA controls>](#) is shown.

The number of controls that are inherited from common controls or other systems is provided where [<inherited controls>](#) is shown.

If there is a deviation request for the system, the following sentence is included and the number of deviations requested is provided where [<deviations>](#) is shown:

A formal deviation request is included to address [<deviations>](#) controls.

Otherwise, the sentence is deleted.

3 MEMORANDUM REFERENCES AND DISTRIBUTION

This memorandum must reference any tickets, especially any issued by the Office of the Executive Director for Operations.

Memorandum distribution must include all office RIDS mailboxes for all offices referenced.

CSO-TEMP-2019 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
13-Jul-10	1.0	Initial release	Posting to CSO web page and notification to ISSOs.	Upon request
30-Jun-14	2.0	Changed to follow new NIST guidance regarding authorizations	Posting to CSO web page and notification to ISSOs.	Upon request

Attachment

System Authorization Package Transmittal Memo for SUNSI Systems



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555 - 0001

<Memo Date>

MEMORANDUM TO:

Darren B. Ash
Deputy Executive Director
for Information Services
and Chief Information Officer
Office of the Executive Director for Operations

Michael R. Johnson
Deputy Executive Director for Reactor
and Preparedness Programs
Office of the Executive Director for Operations

Michael F. Weber
Deputy Executive Director for Materials, Waste,
Research, State, Tribal, and Compliance Programs
Office of the Executive Director for Operations

FROM:

<System Owner Firstname X. Lastname>, Director
<Office or Region Name>

SUBJECT:

REQUEST FOR AUTHORIZATION TO OPERATE <SYSTEM
NAME>

This memorandum constitutes my formal request for an authority to operate for the [<Subsystem Name> (<Subsystem Acronym>) of the] <System Name> (<System Acronym>). A security assessment of the U.S. Nuclear Regulatory Commission (NRC) <Subsystem/System Acronym> and its constituent subsystem-level components (if applicable) has been conducted

CONTACT: <Contact Firstname X. Lastname> <Office or Region Name>
Telephone number (<XXX-XXX-XXXX>)

Enclosures:
As stated

cc: J. Flanagan, OIS
T. Rich, CSO
K. Lyons-Burke, SITSO
T. Graham, SITSO

in accordance with Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems; and NRC policy.

<Subsystem/System Acronym> is categorized as a <System Security Categorization Level> (confidentiality of <low, moderate, high>, integrity of <low, moderate, high>, availability of <low, moderate, high>) sensitivity Information Technology System. Classified information and Safeguards information processing are not permitted.

The enclosed system security authorization package contains:

Document Title	Accession Number
<System Acronym> Business Impact Analysis	<Accession Number>
<System Acronym> Contingency Plan	<Accession Number>
<System Acronym> Deviation Request Memorandum	<Accession Number>
<System Acronym> Deviation Request Spreadsheet	<Accession Number>
<System Acronym> Information System Security Officer Appointment Letter	<Accession Number>
<System Acronym> Interconnection Security Agreement for Interfacing Systems	<Accession Number>
<System Acronym> Memorandum of Understanding for Interfacing Systems	<Accession Number>
<System Acronym> Plan of Actions and Milestones	<Accession Number>
<System Acronym> Privacy Threshold Analysis	<Accession Number>
<System Acronym> Privacy Impact Assessment	<Accession Number>
<System Acronym> Security Categorization	<Accession Number>
<System Acronym> Security Risk Assessment	<Accession Number>
<System Acronym> Service Level Agreement Between Systems	<Accession Number>
<System Acronym> System Security Assessment Plan	<Accession Number>
<System Acronym> System Security Assessment Report	<Accession Number>
<System Acronym> System Security Plan	<Accession Number>
<System Acronym> Vulnerability Assessment Report	<Accession Number>

The security controls listed in the system security plan have been assessed by <Security control assessor> using the assessment methods and procedures described in the System Security Assessment Plan to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Of the <controls assessed> NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations security controls assessed, <in place controls> were found to be in place, <partial controls> were found to be partially in

D. Ash, et. al

-3-

place, <planned controls> are planned, <NA controls> were found to be not applicable, and <inherited controls> were found to be fully inherited at the agency level or from another system. [A formal deviation request is included to address <deviations> controls.] The plan of action and milestones describes the corrective measures that will be implemented to address any deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.

Further, as the system owner, I certify that I or my staff have reviewed the Security Assessment Report and concur with its findings and assert that the security controls provide adequate protection for the information in the system, and that the residual risk of operating the information system is acceptable.