# Nuclear Regulatory Commission
# Computer Security Office
# Computer Security Template

---

| | |
|---|---|
| Office Instruction: | CSO-ADM-5002 |
| Office Instruction Title: | Authority to Operate Memo Template for SUNSI Systems |
| Revision Number: | 1.1 |
| Effective Date: | May 1, 2014 |
| Primary Contacts: | Kathy Lyons-Burke, SITSO |
| Responsible Organization: | CSO/PST |
| Summary of Changes: | CSO-ADM-5002, “Authority to Operate Memo Template for SUNSI Systems” provides the template that must be used to prepare the memo to be issued by the Designated Approving Authority to the system owner that provides the system authorization decision for sensitive unclassified non-Safeguards information systems. |
| Training: | Upon Request |
| ADAMS Accession No.: | ML14107A414 |

| **Concurrences** | | | |
|---|---|---|---|
| **Primary Office Owner** | Policy, Standards, and Training | | |
| **Responsible SITSO** | Kathy Lyons-Burke | | **Date of Concurrence** |
| **Directors** | CSO | Thomas Rich **/RA/** | 21-Apr-14 |
| **Other Stakeholders** | PCT | Kathy Lyons-Burke**/RA/** | 17-Apr-14 |
| | CSA | Thorne Graham **/RA/** | 25-Apr-14 |

| **Concurrence Meeting Conducted via email** | | | |
|---|---|---|---|
| Attendees: | Thomas Rich | Kathy Lyons-Burke | Thorne Graham |
| | | | |

# Computer Security Template
# CSO-ADM-5002

Authority to Operate Memo Template for SUNSI Systems

---

## 1 PURPOSE

The purpose of CSO-ADM-5002, "Authority to Operate Memo Template for SUNSI Systems" is to provide the template that must be used to prepare the memo to be issued by the Designated Approving Authority to the system owner that provides the system authorization decision for sensitive unclassified non-Safeguards information systems.

The title page, purpose, template instructions, and change history are specific to this template office instruction and should be removed from the final memorandum.

## 2 TEMPLATE INSTRUCTIONS

The template sections are completed by the CSO. Information in <blue> in the template should be replaced with the required information and the font color returned to black before submitting the memorandum.

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

The system owner's first name, middle initial, and last name are provided where <System Owner First Name Initial Last Name> is shown.

The 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, and the system acronym is placed wherever <System Acronym> is shown.

A brief description of how NRC will use the system is provided where <system purpose description> 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 includes the confidentiality, integrity, and availability breakout of the overall value. The breakout is provided where <low, moderate, high> is shown.

The first name and last name and the team acronym of the CSO staff member responsible for the CSO system authorization analysis is provided where <CSO Staff Name, CSO/Team> is shown. That staff member's telephone number is provided where <301-415-XXXX> is shown.

The second page header provides the first initial and last name of the system owner where <System Owner First Initial Last> is shown.

The security documentation table identifies required documentation that must be reviewed and referenced before a recommendation can be made. 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 |
|---|---|
| Privacy Impact Assessment (PIA) | Required |
| Information System Security Officer Appointment Letter | Required |
| Security Categorization | Required |
| Security Risk Assessment (SRA) | Required |
| System Security Plan (SSP) | Required |
| Memorandum of Understanding (MOU) for Interfacing Systems | Mandatory for interfaces with external systems; Optional for interfaces with internal systems |
| Service Level Agreement (SLA) between systems | Mandatory for services provided by/for external systems; Optional for services provided by/for internal systems |
| Interconnection Security Agreement (ISA) for Interfacing Systems | Mandatory for interfaces with external systems; Optional for interfaces with internal systems |
| Security Test and Evaluation (ST&E) Plan | Required |
| ST&E Report | Required |
| Vulnerability Assessment Report (VAR) | Required |
| Plan of Actions and Milestones | Required |
| Deviation Request Memorandum | Required |
| Deviation Request Enclosure | Required |
| Business Impact Analysis (BIA) | Required |
| Contingency Plan (CP) | Required |

Any system-specific conditions associated with the ATO are listed in a numbered list where <System-Specific Conditions> is shown. This list should be the same as the one used in the Chief Information Security Officer (CISO) authorization recommendation except where the Designated Approving Authority (DAA) has made modifications.

# 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-ADM-5002 Change History**

| Date | Version | Description of Changes | Method Used to Announce & Distribute | Training |
|---|---|---|---|---|
| 20-Feb-14 | 1.0 | Initial release | Posting to CSO web page and notification to ISSOs. | Upon request |
| 28-Apr-14 | 1.1 | Updated to reflect issues identified by the OEDO | Posting to CSO web page and notification to ISSOs. | Upon request |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Attachment

# Authority to Operate Memo Template for SUNSI Systems

**UNITED STATES**
**NUCLEAR REGULATORY COMMISSION**
**WASHINGTON, DC 20555 - 0001**

<Memo Date>

MEMORANDUM TO: <System Owner First Name Initial Last Name>, Director
<Office or Region Name>

FROM: Darren B. Ash
Deputy Executive Director
for Corporate Management
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

SUBJECT: AUTHORITY TO OPERATE THE <SYSTEM NAME> SYSTEM

This memorandum authorizes operation of <System Name> (<System Acronym>). <System Acronym> <system purpose description>. In support of authorization, the <System Acronym> security authorization package was developed, a security control assessment was conducted, and a Security Assessment Report (SAR), (<Accession Number>), was produced.

<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.

CONTACT: <CSO Staff Name, CSO/Team>
<301-415-XXXX>

cc:
Kathy Lyons-Burke, CSO
Thorne Graham, CSO
Glenda Somerville, CSO

The following table identifies the system security documentation that was reviewed.

| Document Title | Accession Number |
|---|---|
| Privacy Impact Assessment (PIA) | <Accession Number> |
| Information System Security Officer Appointment Letter | <Accession Number> |
| Security Categorization | <Accession Number> |
| Security Risk Assessment (SRA) | <Accession Number> |
| System Security Plan (SSP) | <Accession Number> |
| Memorandum of Understanding (MOU) for Interfacing Systems | <Accession Number> |
| Service Level Agreement (SLA) between internal systems | <Accession Number> |
| Interconnection Security Agreement (ISA) for Interfacing Systems | <Accession Number> |
| Security Test and Evaluation (ST&E) Plan | <Accession Number> |
| ST&E Report | <Accession Number> |
| Vulnerability Assessment Report (VAR) | <Accession Number> |
| Plan of Actions and Milestones (POA&M) | <Accession Number> |
| Deviation Request Memorandum | <Accession Number> |
| Deviation Request Enclosure | <Accession Number> |
| Business Impact Analysis (BIA) | <Accession Number> |
| Contingency Plan (CP) | <Accession Number> |

After reviewing the above system security documentation, its constituent system-level components, the supporting evidence provided in the SAR, the deviation request, and the recommendation of the Chief Information Security Officer, we have determined that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is acceptable. The SAR identifies the required SSP modifications, as well as additions or modifications to weaknesses in the system POA&M.

Accordingly, we are issuing an Authority to Operate (ATO) for <System Acronym> in its existing operating environment. The information system is authorized to operate without any significant restrictions or limitations. This security authorization is our formal declaration that adequate security controls have been implemented in the information system in its existing location and that a satisfactory level of security is present. This security authorization will remain in effect as long as the System Owner satisfies their annual Reasonable Assurance Certification, the periodic assessments of security controls do not reflect an increase in an unacceptable level of risk, and the general and system-specific conditions provided below are met.

**General Conditions**

1) The SSP must be updated within 60 days from the date of this authorization memorandum to reflect findings from the SAR and its Errata, and any approved Deviation Requests.

2) Continuous monitoring and scanning must be performed in accordance with the most recent Cybersecurity Security Risk Management Activities (CSRMA) memorandum, issued by the Executive Director for Operations (EDO), to identify, prioritize, and mitigate system risk.

3) Independent annual security control and vulnerability testing must be funded and conducted, and the SSP must be updated within 60 days of testing.

4) The system CP test must be completed annually within one year of the previous test, and the updated CP and test report must be placed in ADAMS within 60 days of testing.

5) Weaknesses listed in the System-specific Conditions must be added to the system POA&M.

6) All weaknesses (including those identified in the SAR) must be remediated in accordance with the schedule detailed in the updated POA&M.

7) The status of each identified weakness must be updated within the Xacta tool by the 15th of each of the following months: November, February, May and August.

8) The system must be protected against malicious code according to the Computer Security Office (CSO) guidance CSO-GUID-0016, Malicious Code Guidance.

9) The Designated Approving Authority and the Chief Information Security Officer (CISO) must be informed of any risks that impact the system security posture.

10) The System Owner must obtain a system reauthorization upon any significant change to the system.

11) The System Owner must obtain approvals for non-significant changes by submitting a Security Impact Analysis to the CISO.

12) All specific findings identified in periodic reviews must be incorporated into the system security documentation in accordance with the most recent CSRMA memorandum.

13) The Office of Information Services must be notified of the operational status of the system within 30 days of any change affecting the official NRC system inventory record.

14) The system POA&M must be updated in accordance with CSO-PROS-2016, Plan of Action and Milestones Process.

**System-Specific Condition(s)**

1) <System-Specific Conditions>