Nuclear Regulatory Commission Office of the Chief Information Officer
Cybersecurity Oversight and Enterprise Architecture Branch

Office Instruction	**EA-PROS-0100**
Office Instruction Title	**NRC Systems and Services Inventory Process**
Version Number	**1.3**
Effective Date	**January 1, 2021**
Primary Contact	**Garo Nalabandian**
Responsible Organization	**COEAB**
Description	EA-PROS-0100, “NRC Systems and Services Inventory Process,” details the process for identifying/managing and tracking inventory data for systems and services used by the NRC. This process does not include the individual hardware/software items that support systems and services
Office Owner	
Primary	**Agency Official**
COEAB	**Garo Nalabandian** **Deputy CISO**

Table of Contents

Enterprise Architecture Process EA-PROS-0100

NRC Systems and Services Inventory Process

1 PURPOSE

EA-PROS-0100, “NRC Systems and Services Inventory Process,” provides the Nuclear Regulatory Commission (NRC)-approved process that must be followed for identifying/managing and tracking the agency’s inventory data for NRC systems and services (internal and/or external) that enable the NRC to achieve its mission and to meet various federal reporting/metric requirements. The Federal Information Security Modernization Act (FISMA) requires federal agencies to report the status of their information security programs to OMB and requires Inspectors General (IG) to conduct annual independent assessments of those programs. OMB and the Department of Homeland Security (DHS) collaborate with interagency partners to develop the Chief Information Officer (CIO) FISMA metrics, and with IG partners to develop the IG FISMA metrics to facilitate these processes. All federal agencies submit their metrics into the DHS CyberScope on a quarterly basis. The FISMA metrics leverage the Cybersecurity Framework as a standard for managing and reducing cybersecurity risks, and they are organized around the framework’s five functions: Identify, Protect, Detect, Respond, and Recover. The goal of the Identify metrics section is to assist federal agencies with their inventory of the hardware and software systems and assets that connect to their networks. Identifying these systems and assets helps agencies facilitate their management of cybersecurity risks to systems, assets, data, and capabilities.

This process applies to unclassified systems and services and Safeguards Information (SGI) systems. The Office of Nuclear Security and Incident Response (NSIR), Division of Security Operations, is responsible for identifying/managing and tracking classified system inventory.

2 GENERAL REQUIREMENTS

The federal requirements that agencies must abide by have evolved over the years. The Clinger-Cohen Act of 1996 introduced the Capital Planning and Investment Control (CPIC) process for managing major information technology (IT) investments. The CPIC process provides the Chief Information Officer (CIO) with the technical and business value analyses necessary for selecting and monitoring the performance of the agency's IT investments.

Title III of the E-Government Act, entitled the Federal Information Security Modernization Act (FISMA) as amended, provides modifications that modernize federal security practices to address evolving security concerns. These changes strengthen the use of continuous monitoring in systems and increase focus on the agencies for compliance and reporting that is more focused on the issues caused by security incidents.

FISMA, along with the Clinger-Cohen Act, explicitly emphasizes a risk-based policy for cost- effective security. The Office of Management and Budget (OMB) developed Circular A-130, “Managing Information as a Strategic Resource” to support and reinforce this legislation. OMB Circular A-130 was created in 1985 and revised several times; most recently in 2016 as amended requires federal agencies to establish a comprehensive approach to improving the acquisition and management of information resources and to plan for security. This requires an IT investment management process that links to and supports budget formulation and execution while managing risks and returns.

The NRC's FISMA compliance processes address these federal requirements, which includes accounting, managing, and protecting privacy data.

3 SPECIFIC REQUIREMENTS

The NRC connects planning, budgeting, investment management, and architecture disciplines within an integrated solution to provide visibility and control over the agency’s IT system and service inventory.

An information system is the integrated set of components and communication technology owned or operated on behalf of the NRC to support mission/business processes.

An IT service is based on the use of IT and technical expertise to support the agency’s business processes.

At the NRC, IT services are divided into three categories:

- **External** – Systems/services that are operated for or on behalf of the NRC by non-NRC organizations (i.e., Microsoft, Amazon, Office of Personnel Management, Department of Treasury, CGI).
- **Internal** – Systems/services that support the agency that are fully contained within an NRC facility (on premise).
- **Public Facing Web Applications** – Services that represent public facing Web applications that are operated for or on behalf of the NRC.

3.1 System and Service Inventory

There are several pathways where an enhancement to an existing system/service or a new system/service is introduced and accounted for in the NRC environment. Ultimately, the system/service is tracked within the system/service inventory. This includes, but is not limited to, the following:

- **NRC CPIC Process** – The CPIC process assists with managing the overall process to review and approve IT requests initiated by the system/service owners. An NRC user submits a request via service catalog which gets added to the Triage queue in the Remedy tool. Once a week, a technical/cyber review occurs and then goes to appropriate review boards (i.e., architectural and funding) for consideration. Once the request has

been processed and funding is approved, the Requestor gets notified along with the Enterprise Architecture (EA) Branch via email. The custodian then enters the available data into the NRC's system and service inventory located in SharePoint.

- **NRC Configuration Control Board (CCB) Process** – The CCB has the authority to approve minor or selected moderate system/service changes on behalf of the authorizing official. Once approved, the Computer Security Organization (CSO) Point of Contact (POC) notifies the EA system and service inventory custodian of the new or enhanced system/service that needs to be added to the inventory via email at CSO_Inventory@nrc.gov
- **NRC Authorization Processes** – During the authorization process for a new system/service (or significant or selective moderate changes to a system or service), the CSO POC notifies the EA system and service inventory custodian of the new or enhanced system/service that needs to be added to the inventory via email at CSO_Inventory@nrc.gov
- **NRC Privacy Program** – The NRC OCIO Privacy Team provides guidance and direction to ensure IT systems consider privacy protections and controls when making business decisions involving the collection, use, sharing, retention, disclosure, and destruction of personally identifiable information (PII), whether in paper or electronic form.
- **Individual System/Service CCB Processes** – For individual system/service CCB approvals, the system Information System Security Officer (ISSO) works with the CSO POC during the effort. The individual system/service CCB has the authority to approve all changes to systems/services that are not third-party offered cloud services or not directly connected to the NRC Production and Operating Environment. In addition, all moderate changes approved by the board must be approved by the Chief Information Security Officer (CISO). The CSO POC notifies the EA system and service inventory custodian of the new or enhanced system/service that needs to be added to the inventory via email at CSO_Inventory@nrc.gov
- **NRC CSO POC** – The NRC CSOPOC notifies the EA system and service inventory custodian of any other system/service efforts that are not accounted for in the processes listed above via email at CSO_Inventory@nrc.gov

No matter the pathway, the system owner or ISSO must determine the information types processed, stored, or transmitted within the system/service. The types must be reviewed and approved by the CISO and the NRC Privacy Officer before the system/service can be implemented in the NRC environment.

Once the approval is issued, a unique inventory identification (ID) number must be assigned to the system/service for tracking purposes. The ISSO must email the CSO_Inventory@nrc.gov and request a number. The following information must be completed with the email request.

- Name:
- Short Name (abbreviation, acronym, etc.; ideally unique):

- Description:
- Office (acronym of owning NRC office):
- Inventory Type (System, Subsystem, Service, Public/External facing WEB App, Application, etc.)
- System Boundary (acronym of parent system boundary; can be itself)
- Operated by (Contractor NRC, FedRAMP, other Government)

3.2 System and Service Inventory Location

The NRC System and Service inventory list is located on the NRC SharePoint site at the following link:

https://usnrc.sharepoint.com/teams/test-cso-memo/lists/system%20inventory/all%20data%20fields.aspx?skipSignal=true

The SharePoint list provides a flexible way to organize the inventory data. The information can be filtered and or sorted to support information gathering. System and Service Inventory Layout

The following table describes the data fields in the inventory.

Field Names	Existing Values in Inventory	Field Descriptions	Field Owner (security, privacy, EA, Records)
EA_Data_Class_Type	Secret SGI SUNSI Top Secret	Secret SGI SUNSI Top Secret	EA
EA_Description		A description of the Inventory item, including the business purpose or the business process(es) it supports	EA
EA_FEA_Bus_Function	Administrative Management Atomic Energy Defense Activities Central Fiscal Operations ***long list	Lines of business or areas of operation described in 800-60. It is based on the OMB Federal enterprise Architecture Program Management consolidated reference model	EA
EA_FEA_Serv_Name	Accounting Budget formulation Budget Execution	These are subfunctions underneath lines of business	EA
EA_Full_Name	Prepopulated list	The full name of the inventory item	EA
EA_Inv_State	Active Cancelled Development Excessed Inactive N/A Pending	The state of the inventory record such as active, inactive, decommissioned, excessed, pending	EA

Field Names	Existing Values in Inventory	Field Descriptions	Field Owner (security, privacy, EA, Records)
	Replaced Retired		
EA_Inv_Type	Application Building System Facility N/A Operating Environment Placeholder Prototype Public/external facing web app Scientific code Security Hardware Service Social Media Subsystem System Technology item	Subsystem System Public/External facing WEB App Application Social Media On-demand self-service Building System Facility Operating Environment Placeholder Prototype Scientific Code Security Boundary Security Hardware Technology Item N/A Privacy Component?	EA/Security
EA_Number	Populated list	EA Number	EA
EA_Office	Prepopulated list	The initials/acronym of the name of the office that owns the inventory item or has primary responsibility for it	EA
EA_Oper_By	NRC Other Govt Contractor Cloud N/A	Pick List	EA/Security
EA_Short_Name	Prepopulated Acronyms	A short version of the inventory item's name, in the form of an abbreviation, acronym, or initials	EA
PRV_Appr_Date	Approved Dates	Date of most recent approval.	Privacy
PRV_DATA_Found	No Yes	Pick List	Privacy
PRV_Date Last_Reviewed	Date options are provided	Date last PIA/PTA was reviewed	Privacy
PRV_Govt_SORNS	PIC List of government wide SORNS used by NRC.	PIC List of all government wide SORNS used by NRC	Privacy
PRV_ML_Num	Prepopulated ML #s	ML number of the PIA	Privacy
Prv_NRC_SORNS	Prepopulated list of names	Drop down listing of all NRC SORNs	Privacy
PRV_OMB_Clear_Num	Clearance not needed NRC Forms 850A	OMB clearance numbers	Privacy
PRV_PII_Types	Fillable Text	Types of PII (e.g. SSN, home address, telephone number)	Privacy
PRV_Records_Retention	Yes No		Privacy
PRV_Reviewer	Fillable Text	Name of person who completed the last PIA/PTA review	Privacy

Field Names	Existing Values in Inventory	Field Descriptions	Field Owner (security, privacy, EA, Records)
Prv_SORNS	Yes No Unknown		Privacy
PRV_SSN_Found	Yes No Partial Full	SSNs Found ? (Yes / No)	Privacy
PRV_Type	PTA PIA	Pick List	Privacy
RM_Activity	Multiple lines of text	Spells out specific activities within each Information Business Function that NRC performs, such as Legal Investigations or Docket Files.	Records
RM_Category	Multiple lines of text	Represents which of the five broad line of business categories at NRC - Organizational Support, Mission Support, Licensing, Oversight & Inspections, and Research - that the records series would fall under. There are interdependencies between the CFAs. See file categorizations sheet or contact IM Policy Team for assistance. Most CFA's have been approved by offices based on the records schedules in NUREG 0910.	Records
RM_File_Location	Multiple lines of text	Include if in multiple storage locations (physical and/or electronic) and in a system(s). Provides the location where the information is stored, such as ADAMS, shared drive (G: drive), a specific system/database (e.g. FAIMIS), file cabinet, SharePoint, etc.	Records
RM_Function	Multiple lines of text	Represents which of the sub-categories within each line of business that the records series would fall under, such as Nuclear Incident Response or Outreach & Public Relations.	Records
RM_Media	Multiple lines of text	Include if in multiple formats and locations and what format in system(s). Shows what type of media on which the information is stored. Examples of media types include electronic, paper, magnetic tape, system/database, DVD, video, prints & negatives, microfilm, audio cassette, etc.	Records
RM_Permanent_Temporary	Multiple lines of text	States if the document should be transferred to NARA after a certain period of time for permanent holding or if the	Records

Field Names	Existing Values in Inventory	Field Descriptions	Field Owner (security, privacy, EA, Records)
		information has a disposition that allows it to be destroyed at some point in the future (Temporary). Note: temporary retention periods could be almost any amount of time, from 1 month to 10,000 years. If (and, only if) a record ends up at NARA according to the disposition instruction – it is "permanent." All other records are "temporary." Also refer to NUREG 0910 instruction.	
RM_Records_Series_Name	Multiple lines of text	Provides the name of the records series, such as "Communications – Internal Communications" or "Time and Attendance Records". These descriptions come directly from the Records Schedules unless records are unscheduled.	Records
RM_Schedule_Number	Multiple lines of text	Numbers represent: General Records Schedule (GRS) – schedules issued by NARA to provide disposition authorization for records common to several or all agencies of the Federal Government and; NUREG-0910, NRC Comprehensive Records Disposition Schedule" -NRC schedules that provide the authorized disposition for all NRC records, after being approved by NARA. Application of the disposition schedules is mandatory for all scheduled records, and unscheduled records must be held until a disposition authority is obtained.	Records
RM_Series_Description	Multiple lines of text	These Series Descriptions come directly from the Records Schedules unless records are unscheduled. Provides a general description of what type of information and documents would be contained in a series, e.g., for a records series named "Records Disposition Files," the series states that it includes "descriptive inventories, disposal authorizations, schedules, and reports." Descriptions also provide additional information for a series that has multiple categories. For example, within	Records

Field Names	Existing Values in Inventory	Field Descriptions	Field Owner (security, privacy, EA, Records)
		the “General Program Correspondence Files (Subject Files)” records series, it contains three sub-series: 1) Program Correspondence Files at the Office Director Level; 2) Program Correspondence Files below the Office Director Level; and 3) Routine Program Correspondence Files.	
RM_Vital_Business_Info_Locator	Multiple lines of text	States if a record is considered a piece of VBI, which would be required in order to resume business in the event that a disaster occurs, and the agency utilized its Continuity of Operations (COOP) plans. Are these records part of the organization’s Vital Business Information (VBI)?	Records
SEC_Alt_ISSO	Drop down list with prepopulated names	The name of the first alternate information system security officer (ISSO)	Security
SEC_Alt_ISSO_Appt_Date	Date options are provided	Date of appointment	Security
SEC_Auth_Date	Date options are provided	The date an inventory record is authorized	Security
SEC_Auth_Exp_Date	Date options are provided	The date when the accreditation of the system is no longer valid.	Security
SEC_Auth_Type	Expired ATT Authority to operate Decommissioned In development Not applicable Ongoing Periodic Short term	The type of security authorization for this inventory item	Security
SEC_Bus_Owner	No values	Technical POC for TPS subsystems	Security
SEC_Cloud_Deploy_Model	Community Hybrid Public Private N/A	Deployment models are defined according to where the infrastructure for the environment is located (i.e., private, community, public, hybrid and government).	Security
SEC_Cloud_Service_Model	IaaS PaaS SaaS N/A	The type of model (IaaS, PaaS, SaaS) used by NRC	Security
SEC_Comments		Various status notes-wide ranging comments	EA
SEC_CSO_POC	Alan Sage Bill Bauer Bill Dabbs Nicole Crouch Mike Mangefrida	Pick list	Security
SEC_Ext_Service_Type	Other Govt Cloud/FedRAMP	A view for external IT services would filter on this field and	Security

Field Names	Existing Values in Inventory	Field Descriptions	Field Owner (security, privacy, EA, Records)
	Contractor Hybrid NRC	include everything but the NRC. A view for internal services would filter on NRC only or hybrid.	
SEC_Ext_Srv_Provider	Fill in	Name of the Agency or Name of the contractor. Cloud Provider utilizes its own dedicated field.	Security
SEC_FedRAMP_ATO_Letter	Yes / No	If the inventory record has an ATO letter on file at FedRAMP PMO	Security
SEC_FedRAMP_Auth_Type	Agency Jab	Authorized FedRAMP Cloud service. If it is not authorized leave blank.	Security
SEC_FedRAMP_Srv_Offer	Fillable fields such as; Azure Commercial Cloud Office 365 Multi-tenant AWS US E/W AWS Gov Cloud	Name of the offering used by NRC Such as: Azure Commercial Cloud Office 365 Multi-tenant AWS US E/W AWS Gov Cloud	Security
SEC_FedRAMP_Srv_Provider	Fillable Field such as: Amazon MicroPact Microsoft Oracle Amazon University Central Florida	Fillable Text	Security
SEC_FIPS_199_A	Low Moderate High	The FIPS 199 categorization of the potential impact due to loss of availability (A)	Security
SEC_FIPS_199_C	Low Moderate High	The FIPS 199 categorization of the potential impact due to loss of confidentiality ©	Security
SEC_FIPS_199_I	Low Moderate High	The FIPS 199 categorization of the potential impact due to loss of integrity (I)	Security
SEC_FIPS_199_O	Low Moderate High	The overall FIPS 199 categorization, which is the highest impact value among FIPS 199 A, FIPS 199 C, and FIPS 199 I.	Security
SEC_HVA_Alt_Pros_Site	N/A R4 Ashburn	Pic List of alternate processing site locations used at the NRC.	Security
SEC_HVA_Connect_Ext_Entity	Yes No	Is the HVA connected to an external entity	Security
SEC_HVA_Connect_Int_Entity	ITI BASS ACCESS OCIMS ADAMS	What HVA interconnects to internally	Security
SEC_HVA_Fail_Time_Impact	<1 Hour <1 Week	Pick List	Security

Field Names	Existing Values in Inventory	Field Descriptions	Field Owner (security, privacy, EA, Records)
	<1 Month >1 Month		
SEC_HVA_How_Many_PMEF	Number	Fillable Text. Primary Mission Essential Functions (PMEFs) are those functions that need to be continuous or resumed within 12 hours after an event and maintained for up to 30 days or until normal operations can be resumed. PMEFs are validated by the Federal Emergency Management Agency (FEMA) National Community Coordinator.	Security
SEC_HVA_MEF	MEFs HVA supports	Fillable Text. Agency level government functions that must be resumed rapidly after, a disruption of normal operations. MEFs are functions that cannot be deferred during an emergency or disaster.	Security
SEC_HVA_PMEF	PMEFS HVA supports	Fillable Text.	Security
SEC_HVA_Tier	N/A Tier 1 Tier 2	Is the system categorized as an HVA Yes or No	Security
SEC_Prim_ISSO	Prepopulated list	The name of the appointed Primary Information System Security Officer	Security
SEC_Prim_ISSO_Appt_Date	Prepopulated dates	The date that the Information System Security Officer was appointed.	Security
SEC_PUB_Facing	Yes No NA	Pick List	Security
SEC_Sub_Sys	Prepopulated Acronyms	Name of the subsystem	Security
SEC_System_Boundary	Prepopulated with FISMA System Names	FISMA system boundary of the inventory item	Security
SEC_System_Owner	Office Director OCIO Division Director Regional Administrators e.g. OCHCO, OCIO/SDOD, Region III	Name of the individual responsible for the overall procurement, development, integration, security, operation, maintenance, and retirement of an information system.	Security

Currently, there are 4 field owner roles:

- Enterprise Architecture (EA)
- Security
- Privacy
- Records

The field owner has sole authority to change the field name, description, or value.

The following views have been created for efficiency and to meet the various reporting requirements for which the NRC is responsible. These views limit the fields that appear to support the specified information need.

- FISMA Systems
- FISMA Subsystems
- Public Facing Web Apps
- External IT Services
- Expired Authorizations
- High Valued Asset (HVA)
- Privacy
- Records
- CyberScope

3.3 Maintaining the Inventory

The NRC Risk and Continuous Authorization Tracking System (RCATS) interfaces with the SharePoint Inventory List to update the following fields on a nightly basis:

- SEC_Auth_Date
- SEC_Auth_Exp_Date
- SEC_Auth_Type
- SEC_FIPS_199_C
- SEC_FIPS_199_I
- SEC_FIPS_199_A
- SEC_FIPS_199_O
- EA_Number
- EA_Office
- PRV_Type
- PRV_PII_Types
- SEC_Prim_ISSO
- EA_Short_Name
- SEC_Sub_Sys
- SEC_System_Names
- SEC_System_Owner

On a bi-monthly basis, security and privacy field owners meet to discuss any updates that need to be made to the inventory based on changes that have occurred. Adhoc/structural updates to the inventory must be coordinated by email to CSO_Inventory@nrc.gov.

Annually, the system and service inventory is independently verified by an enterprise assessor. A high-level test plan is developed prior to the assessment that describes the testing approach and scope. A test report is created by the enterprise assessor that documents the discrepancies and weaknesses discovered during the assessment. Corrective actions are taken to correct any discrepancies.

3.4 Decommission System/Service and/or Transfer

When a system/service is transferred to another system becomes obsolete, or is no longer usable, proper decommissioning must be followed for proper inventory accountability. Once approval for the decommissioning and/or transfer of the system/service has been obtained, the ISSO must email CSO_Inventory@nrc.gov so the inventory can be updated to reflect the status.

Refer to CSO-PROS-2101, “NRC IT System/Subsystem/Service Decommissioning and/or Transfer Process,” for more information on this process.

APPENDIX A. REFERENCES

System documentation repositories, policies, and processes related to FISMA activities are provided in the CSO FISMA Repository at:

https://usnrc.sharepoint.com/teams/OCIO-CSO/SitePages/Home.aspx

- CSO-PROS-1323, “Information Security Continuous Monitoring Process,”
- CSO-PROS-1341, “Short-Term Change Authorization Process,”
- CSO-PROS-2001, “System Security Categorization Process,”
- CSO-PROS-2101, “NRC IT System/Subsystem/Service Decommissioning and/or Transfer Process,”
- CSO-PROS-2102, “System Cybersecurity Assessment Process,”

EA-PROS-0100 Change History

Date	Version	Description of Changes	Method used to Announce & Distribute	Training
12/18/2019	1.0	Initial release	OCIO/CSO website	As Needed
12/11/2020	1.1	Phase 2 Updates	OCIO/CSO website	As Needed
4/14/2021	1.2	Minor edits made to inventory fields table	OCIO/CSO website	As Needed
5/5/2021	1.3	Added language in Section 3 to clarify definitions of an external, internal and public facing web application	OCIO/CSO website	As Needed