Minimum Required Frequencies for Continuous Monitoring Activities Defined in CSO-PROS-1323

All continuous monitoring submissions must be sent to the CSO-FISMA-Submittals@nrc.gov, CISO, and CSO Office POC.

Minimum Frequencies for all NRC Systems regardless of System Categorization

#	Activity Name	Frequency	Notes
1.	Business Impact Analysis (BIA)	At least annually - review and update as needed (e.g., if the system has undergone a change that impacts disaster recovery planning). Ideally, prior to the system's contingency test to ensure accuracy of information. Please note: systems with a Low impact level for availability DO NOT have to create/document a BIA.	External IT services (EITS) recovery information can be included in the parent system's BIA. Availability/recovery requirements for Third Party System (TPS) subsystems are defined within the TPS BIA.
2.	Contingency Plan (CP) Update	At least annually - review the system's Contingency Plan and update as needed. Ideally, prior to the system's contingency test to ensure accuracy of information.	EITS CP information can be included in the parent system's CP. Recovery information for TPS subsystems is defined within the TPS CP.
3.	Contingency Plan Training	At least annually - provide training prior to conducting the system's contingency test.	
4.	Contingency Test Plan Update	Must be updated prior to conducting the system's contingency test.	Testing for EITS and TPS will be limited based on NRC responsibilities.
5.	Contingency Test	Annually - must be completed no later than the same quarter as the previous year, or with an Authorizing Official (AO) or CISO-approved delay.	Testing for EITS and TPS will be limited based on NRC responsibilities.
6.	Contingency Plan Test Report	Annually - must be completed no later than the same quarter as the previous year, or with an Authorizing Official (AO) or CISO-approved delay.	
7.	Interconnection Security Agreement (ISA)	This is required between NRC and external entities; not between internal NRC systems. Provide most recent ISA (if any) and confirm terms are reviewed annually and carried out accordingly by June 15.	
8.	Memoranda of Understanding (MOU)	This is required between NRC and external entities; not between internal NRC systems. Provide most recent MOU (if any) and confirm terms are reviewed annually and carried out accordingly by June 15.	

Minimum Frequencies for all NRC Systems regardless of System Categorization

#	Activity Name	Frequency	Notes
9.	ISSO Appointment (System)	Must be identified within 15 business days, of being assigned the role.	
10.	External IT Services MOU/ISA/Authorization Notifications	Notify the AO within 15 business days of an authorization expiration or termination, significant changes, unacceptable risks or any changes to the MOU/ISA.	
11.	Periodic System Cybersecurity Assessment (PSCA)	Annually - must be independently conducted and completed no later than the same quarter as the previous year, or with an AO or CISO-approved delay.	
12.	Plan of Action and Milestones (POA&M) Updates	For NRC systems, quarterly updates are required by December 15, March 15, June 15, and September 15 of each fiscal year.	For EITS and TPS: It is the NRC ISSO's responsibility to review and analyze the CSP's POA&M evidence on monthly basis to ensure mandatory requirements are conducted and meet an acceptable level of risk.
13.	System Security Plan (SSP)	At least annually - review and update as needed to ensure accuracy and account for any changes that have been authorized for the system. Must be dated within one year after the date of the last annual update. Ideally, prior to the PSCA to ensure accuracy of information.	For EITS and TPS: At least annually - review and update as needed (e.g., as needed if the document is impacted by a change to the external IT service and/or NRC responsibilities).

Minimum Frequencies for all NRC Systems regardless of System Categorization

#	Activity Name	Frequency	Notes
14.	Supporting documentation may include but not limited to: • Security Categorization Report • Digital Authentication Risk Assessment Report • Privacy Threshold Analysis/Privacy Impact Assessment • Configuration Management Plan • Incident Response Plan • Documented Configurations • System Inventory • System Architecture Document • Operational Support Procedures	At least annually - review and update as needed to ensure accuracy and account for any changes that have been authorized for the system. Ideally, prior to the PSCA to ensure accuracy of information. After a thorough review, if no changes are necessary, change the version of the document and make an entry in the document revision history stating, "Document reviewed-no updates needed."	Not all supporting documentation will be applicable to EITS and TPS. See Section 5 and 6 in the CSO-PROS-1323 for more information.
15.	Vulnerability Scanning	All systems/subsystems must conduct vulnerability scans once per quarter. In addition to the quarterly vulnerability scanning requirement, system compliance scans and manual checks must be conducted based on the system's security categorization, as follows: High: Semi-annually Moderate: Annually Low: Annually	Applicable to EITS if NRC has responsibility for vulnerability scanning. Not applicable to TPS. If available, system ISSO is responsible for reviewing EITS continuous monitoring scans monthly to ensure it is being conducted and findings are being remediated.

Minimum Frequencies for all NRC Systems regardless of System Categorization

#	Activity Name	Frequency	Notes
16	Wireless Scanning	Annually - if the wireless network only supports guests and only provides connectivity to the Internet (external IP addresses only) Quarterly - if the wireless network allows users to access the NRC internal network or NRC public sites in any way (includes MaaS, Outlook Web Access, Virtual Private Networking, NRC-encrypted guest network and Citrix)	Not applicable to EITS and TPS