Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Process

Office Instruction:	**CSO-PROS-0009**
Office Instruction Title:	**Supply Chain Software Evaluation Process**
Revision Number:	**1.0**
Effective Date:	
Primary Contacts:	**Kathy Lyons-Burke** **Senior Level Advisor for Information Security**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-PROS-0009, “Supply Chain Software Evaluation Process,” defines the process that must be used to evaluate any software that NRC uses.
ADAMS Accession No.:	ML22332A046

Chief Information Security Officer	**Approval Signature and Date**
Jon Feibus for Garo Nalabandian, OCIO/FO	Jonathan R. Feibus Digitally signed by Jonathan R. Feibus Date: 2022.12.22 11:18:38 -05'00'

Table of Contents

Computer Security Process
CSO-PROS-0009
Supply Chain Software Evaluation Process

1 PURPOSE

In accordance with Office of Management and Budget (OMB) Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" [M-22-18], Nuclear Regulatory Commission (NRC) must only use software provided by software producers who can attest to complying with the Government-specified secure software development practices, as described in the National Institute of Standards and Technology (NIST) Guidance [NIST SW SCSG]. CSO-PROS-0009, "Supply Chain Software Evaluation Process," defines the process that must be used to evaluate any software that NRC uses.

2 GENERAL REQUIREMENTS

NRC must only use software provided by software producers who can attest to complying with the Government-specified secure software development practices, as described in the NIST Guidance on secure software development [NIST SW SCSG]. NRC must follow this process to ensure software producers have implemented and will attest to conformity with secure software development practices

This process must be performed by the Computer Security Organization (CSO), in coordination with the Contracting Officer's Representative (COR), and Contracting Officer (CO) for each product and service the NRC currently uses or might use that includes an Information Technology (IT) component, and the results must be stored in a software product and service repository associated with the product or service.

This process must be followed for all NRC use of software developed after September 14, 2022, as well as NRC's use of existing software that is modified by major version changes (e.g., using a semantic versioning schema of Major.Minor.Patch, the software version number goes from 2.5 to 3.0) after September 14, 2022.

A third-party assessment provided by either a certified FedRAMP Third Party Assessor Organization (3PAO) or one approved by NRC shall be acceptable in lieu of a software producer's self-attestation, including in the case of open source software or products incorporating open source software, provided the 3PAO uses the NIST Guidance as the assessment baseline.

This process is not required for agency-developed software.

If NRC awards a contract that may be used by other agencies, NRC is responsible for implementing this process for software that is part of the contract.

3 ROLES AND RESPONSIBILITIES

Table 1 provides the roles and responsibilities associated with supply chain software evaluation.

Table 1: Supply Chain Software Evaluation Roles and Responsibilities

Role	Responsibilities
Office of Administration (ADM) Division of Acquisition Management (AMD) Acquisition Policy, Planning & Support Branch (APPSB)	• Notifies all NRC contractors about the need for software attestation letters. • Ensures that purchase card holders understand the requirement to obtain software attestation letters for all acquisitions that include any IT capability.
Chief Information Security Officer (CISO)	• Determines if information provided in place of a full attestation letter is acceptable.
Contracting Officer (CO)	• Ensures that software attestation requirements are incorporated into all contracts that include any IT capability. • Assists the COR and CSO in obtaining attestation letters for NRC contracts.
Contracting Officer's Representative (COR)	• Works with the CO to assist the CSO in obtaining attestations letters.
Office of the Chief Information Officer (OCIO), Information Technology Services Development and Operations Division (SDOD) Service Fulfillment and Delivery Branch (SFDB) Branch Chief	• Notifies the CSO of any upcoming software major version upgrade and requests that a software attestation letter be obtained. • Ensures NRC has a software attestation letter before a software major version upgrade is implemented.
OCIO CSO	• Determines if a self-attestation letter is available for the company from which the product/service is being acquired. • If a self-attestation letter is not available, works with the COR and CO to obtain from the software producer a document listing those practices to which they cannot attest, documenting practices they have in place to mitigate those risks, and require a Plan of Action & Milestones (POA&M) to be developed. Then, requests CISO review to determine if this information is acceptable. • Works with the COR/requester to obtain a self-attestation letter if needed. • Places all self-attestation information into the software attestation index and software attestations and artifacts folder. • Notifies the COR/requester of the availability of the required software attestation letter.
Purchase Card Holders	• Ensures that an attestation letter is included as part of the Form 30 [Form 30] or equivalent required form.
Requester (if purchase is not via a contract)	• Notifies the CSO of the need for a software attestation letter for any acquisition that includes any IT capability prior to the acquisition. • Ensures that a software attestation letter is obtained for any acquisition that includes any IT capability prior to the acquisition.

Table 1: Supply Chain Software Evaluation Roles and Responsibilities

Role	Responsibilities
	• Provides the attestation letter to the CSO to place in the software attestation index and software attestations and artifacts folder • Includes a link to the attestation letter as part of the Form 30 [Form 30] or equivalent required form.

4 SOFTWARE EVALUATION

A software producer's self-attestation serves as a "conformance statement" described by the NIST Guidance [NIST SW SCSG]. NRC must obtain a self-attestation for all third-party software used by the agency, including software renewals and major version changes.

CSO must ensure that the producer of any software currently in use at the NRC or intended for use at the NRC has attested to complying with the Government-specified secure software development practices, as described in the NIST Guidance [NIST SW SCSG]. Software evaluations for critical software must be prioritized over software evaluations for other software.

4.1 Contracts

ADM/AMD/APPSB sends out a one-time announcement to all current contractors notifying them of the requirement for a software attestation letter that includes a link to the Cybersecurity and Infrastructure Security Agency (CISA) provided standard attestation letter.

Once available, the CO incorporates the Federal Acquisition Regulations (FAR) language that requires the software attestation letter into all contracts initiated after September 14, 2022 that include any IT capability. If there is a lag in finalizing the FAR language, the CO incorporates the requirements using language as directed by the Federal Acquisition Security Council (FASC) and the Office of Federal Procurement Policy (OFPP).

4.2 Purchase Card Acquisitions

A requester for any acquisition that includes any IT capability must include a link to the providers software attestation letter that is located within the software attestation index. The requester notifies the CSO of the need for a software attestation letter for any acquisition that includes any IT capability prior to the acquisition. The CSO supports the requester in locating or obtaining the required attestation letter, and the requester includes a link to the attestation letter as part of the Form 30 [Form 30] or equivalent required form.

Prior to making a purchase card acquisition for anything that includes any IT, the purchase card holder must ensure that NRC has an acceptable software attestation letter for the item being purchased.

4.3 Determining if the Required Attestation is Currently Available

The following steps should be followed to determine if the required attestation is currently available:

1. The CSO checks the supply chain risk management software attestation index to determine if NRC is aware of an attestation.
2. If the producer of the software is not listed in the index, the CSO checks to see if the producer has posted a publicly available attestation. If so, the CSO adds the producer to the attestation index, including the link to the publicly available attestation.
3. The CSO notifies the requester of the availability of the required software attestation letter.

4.4 Obtaining the Required Attestation

The minimum requirements for an acceptable self-attestation are provided in Appendix F. The following steps should be followed to obtain the required attestation:

1. If an attestation is not available, the CSO must obtain the required software attestation letter. The CSO/COR/CO/requester should encourage the software producer to be product inclusive so that the same attestation may be readily provided to all purchasing agencies.
    a. If the acquisition is a contract, the CSO works with the COR and CO to obtain an attestation using the CISA provided standard attestation letter.
    b. If the acquisition is for other than a contract, the CSO works with the requester to obtain an attestation using the CISA provided standard attestation letter.

2. If the software producer cannot attest to one or more practices from the NIST Guidance identified in the standard self-attestation form, the NRC must require the software producer to identify those practices to which they cannot attest, document practices they have in place to mitigate those risks, and a POA&M to be developed.
    a. The agency shall take appropriate steps to ensure that such documentation is not posted publicly, either by the vendor or by the agency itself.
    b. If the software producer supplies that documentation and the CISO finds it satisfactory, NRC may use the software despite the producer's inability to provide a complete self- attestation.
    c. The information provided by the software producer to enable this CISO decision must be placed in the attestation repository and the Software Attestation Index must be updated to include the software producer and the link to the attestation information.

3. **Documentation provided in lieu of a complete self-attestation, as described in the preceding paragraph, shall not be posted publicly by the vendor or the agency.**
4. Once the letter is obtained, the CSO stores the letter in the Software Attestations and Artifacts folder, updates the supply chain risk management software attestation index, and notifies the requester of the availability of the required attestation letter.

4.5 Major Software Upgrade

Prior to any software major version upgrade, the OCIO/SDOD/SFDB Branch Chief notifies the CSO of the need for a software attestation letter that applies to the upgrade. The upgrade may not take place until the attestation letter is obtained.

4.6 Waiver Process

Agencies may request a waiver—only in the case of exceptional circumstances and for a limited duration—for any specific requirement(s) of M-22-18. The waiver request must be submitted to the Director of OMB and must be transmitted 30 days before any relevant deadline in M-22-18 and accompanied by a plan for mitigating any potential risks. The Director of OMB, in consultation with the Assistant to the President and National Security Advisor (APNSA), will consider granting the request on a case-by-case basis.

Specific instructions for submitting requests for waivers will be posted in MAX at this URL: https://community.max.gov/x/LhtGJw.

APPENDIX A ACRONYMS

3PAO	FedRAMP Third Party Assessor Organization
ADM	Office of Administration
AMD	Division of Acquisition Management
APNSA	Assistant to the President and National Security Advisor
APPSB	Acquisition Policy, Planning & Support Branch
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CO	Contracting Officer
COR	Contracting Officer's Representative
CSO	Computer Security Organization
FAR	Federal Acquisition Regulations
FASC	Federal Acquisition Security Council
FO	Front Office
FY	Fiscal Year
IT	Information Technology
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
POA&M	Plan of Action & Milestones
SDOD	Information Technology Services Development and Operations Division
SFDB	Service Fulfillment and Delivery Branch

APPENDIX B REFERENCES

POLICIES, REGULATIONS, DIRECTIVES, AND INSTRUCTIONS

[EO-14028]	Executive Order 14028, Improving the Nation's Cybersecurity, May 12, 2021
[M-22-18]	OMB Memorandum Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, September 14, 2022

STANDARDS, GUIDELINES, AND REPORTS

[CISA SCRM]	CISA Information and Communications Technology (ICT) Supply Chain Risk Management
[NIST CritSW]	NIST Critical Software – Definition and Explanatory Material
[NIST SW SCSG]	NIST Software Supply Chain Security Guidance

NRC DOCUMENTS

[Form 30]	Standard Form 30
[MD 12]	MD 12, "Glossary of Security Terms"
[MD 12.5]	MD 12.5, "NRC Cybersecurity Program"
[Risk strategy]	NRC Risk Management Strategy, Revision 1.0, ML20266G443
[SCRM Strategy]	NRC Supply Chain Risk Management Strategy, Revision 1.0, September 2020, ML20310A085

APPENDIX D GLOSSARY

Conformance Statement	A declaration that identifies with which requirements an implementation meets.
Critical Software	Executive Order 14028 critical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: • is designed to run with elevated privilege or manage privileges; • has direct or privileged access to networking or computing resources; • is designed to control access to data or operational technology; • performs a function critical to trust; or, • operates outside of normal trust boundaries with privileged access.
Major.Minor.Patch	MAJOR version increment indicates incompatible API changes. MINOR version increment indicates addition of functionality in a backwards-compatible manner. PATCH version increment indicates backwards-compatible bug fixes.
Secure Software Development	Software development practices that ensure security is built into the development software. This includes involving people and practices, and ensuring application confidentiality, integrity, and availability.
Self Attestation	A statement by an individual or organization providing a status related to a particular requirement and the signed document stating that status.
Software Producer	An organization that develops software where a licensing system is used to control use of the software.
Versioning Schema	A simple set of rules and requirements to assign and increment version numbers.

APPENDIX F REQUIREMENTS AN ACCEPTABLE SELF-ATTESTATION

An acceptable self-attestation must include the following minimum requirements as defined in M-22-18:

- The software producer's name
- A description of which product or products the statement refers to (preferably focused at the company or product line level and inclusive of all unclassified products sold to Federal agencies)
- A statement attesting that the software producer follows secure development practices and tasks that are itemized in the standard self- attestation form
- Self-attestation is the minimum level required; however, agencies may make risk-based determinations that a third-party assessment is required due to the criticality of the service or product that is being acquired, as defined in OMB M-21-30

CSO-PROS-0009 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
21-Dec-22	1.0	Initial release	Monthly Office Meetings.	None needed.