National Aeronautics and Space Administration

Secure Software Development Self-Attestation Collaboration Opportunity #4

Kanitra Tyler, ICT/C-SCRM Service Element Lead
Kay Twitchell, Deputy Software License & Asset Manager
August 7, 2024

WELCOME

- Please type your name, entity/publisher being represented, and contact email in the chat or email NASA Software Attestation POCs via Agency-DL-SoftwareAttestation@mail.nasa.gov
- Collaboration Opportunities are intended to establish bi-directional communications regarding the self-attestation collection process and answer or clarify any questions from our supplier/contractor & publisher community.
- Unless there are objections, sessions will be recorded

BLUF

The Federal Information Security Modernization Act of 2014 (FISMA) requires each Federal agency to provide security protections for both “information collected or maintained by or on behalf of an agency” and for “information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.”

Consistent with these authorities and the directives of EO 14028, each Federal agency is required to comply with the NIST Guidance when using third-party software on the agency’s information systems or otherwise affecting the agency’s information.

We do anticipate a future contract requirement that is linked to Open Federal Acquisition Regulation (FAR) Case 2023-002 affecting Parts 1, 39, 52.

Agenda

- Announcement - Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle (formerly referred to as The Buyer's Guide) has been published.
- Extensions (cannot attest right now) & NASA's Process
- Waivers (will never attest) & NASA's Process
- NASA Review and Submission of Waivers
- Question & Answer

When a software producer cannot attest…

TLP:GREEN

Extensions—If an agency is using software from a producer who cannot attest by the deadline, there is a pathway to maintain software usage:

- Collect and evaluate:
  - Practices to which they cannot attest;
  - Mitigation of associated risks; and
  - Plan of Actions and Milestones (POA&M)
- Submit an extension request to OMB:
  - OMB may designate the lead agency for coordination purposes

NASA's Process for Submission of Extensions/POA&Ms

- Software publisher responsibility to submit extension/POA&Ms to NASA for software for which the publisher cannot attest to secure software development practice(s) **at this time**; NASA responsibility to submit to the OMB Extensions & Waivers portal
  - ✓ Common Form **and** identified practice(s) that the software publisher cannot attest to associated with the appropriate NIST SP 800-53, Rev. 5 SA and/or SR control(s)
  - ✓ Compensating or mitigating practice(s)
  - ✓ Compensating or mitigating control(s)
  - ✓ Date the Common Form practice(s) will be implemented
- Software publishers should have a reasonable expectation that some form of evidence will be requested/required to close POA&Ms

Please Place a 'X' to Select Common Form Practice [required]	Common Form Practice for which an Extension is Being Requested	Related NIST SP 800-53 Control(s)	Compensating or Mitigating Practice(s) and Control(s) [required]	Date the Common Form Practice will be Implemented [required]	Additional Notes/Information [optional]
	1a, b, c, d & f	SA-3(1), SA-8, SA-15			

When a software producer cannot attest…

TLP:GREEN

Waivers—If an agency is using software from a producer who will never attest:

- Agencies may request a waiver (only in the case of exceptional circumstances and for a limited duration)
- Must be transmitted 30 days before any relevant deadline
- Accompanied by a plan for mitigating any potential risks
- The Director of OMB, in consultation with the Assistant to the President for National Security Affairs (APNSA), will consider granting the request on a case-by-case basis

NASA's Process for Submission of Waivers

- Software publisher responsibility to submit waivers for software for which the publisher will **never** attest to secure software development practice(s); NASA responsibility to submit to the OMB Extensions & Waivers portal
  - ✓ Common Form **and** identified practice(s) that the software publisher will **never** be able to attest to.
  - ✓ Compensating or mitigating practice(s) Risk mitigation plan
- Software publishers should have a reasonable expectation that software will be removed from the NASA environment if they will never be able to attest to following secure software development practices, absent "exceptional justification."
- Please note it is not OCIOs intention to pursue the waiver route, rather, we will pursue an alternative – an exit strategy for software for which a publisher will **never** be able to attest to following secure software development practices, absent "exceptional justification."

Please Place a 'X' to Select Common Form Practice [required]	Common Form Practice that the Software Publisher will NEVER be able to attest	Related NIST SP 800-53 Control(s)	Compensating or Mitigating Practice(s) [required]	Risk Mitigation Strategy(ies) [required]	Additional Notes/Information [optional]
	2	SA-1, SA-3(1), SA-4, SA-5, SA-8, SA-8(3), SA-9, SA-10, SA-10(6), SA-11, SA-15, SA-15(11), SR-3, SR-4, SR-4(3), SR-4(4)			

Resources

- NASA Knowledge Center (internal) – https://nasa.sharepoint.com/sites/ictscrm/SitePages/SCRM-Knowledge-Center(1).aspx
- NASA Knowledge Center (external) – https://www.nasa.gov/supply-chain-risk-management-scrm/
- RSAA - https://softwaresecurity.cisa.gov/login
- RSAA User Guide - https://www.cisa.gov/sites/default/files/2024-03/CISA_RSAA_User_Guide_18_March_2024.pdf
- Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle (formerly referred to as The Buyer's Guide) - https://www.cisa.gov/resources-tools/resources/software-acquisition-guide-government-enterprise-consumers-software-assurance-cyber-supply-chain
- Executive Order 14028 - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- OMB M-22-18 - https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf
- OMB M-23-16 - https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf
- NIST, EO Definition and Categories Explained - https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory
- FedRAMP Recognized 3PAO - https://marketplace.fedramp.gov/assessors
- Proposed FAR Rule - https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=9000-AO49

Q & A

Kanitra D. Tyler

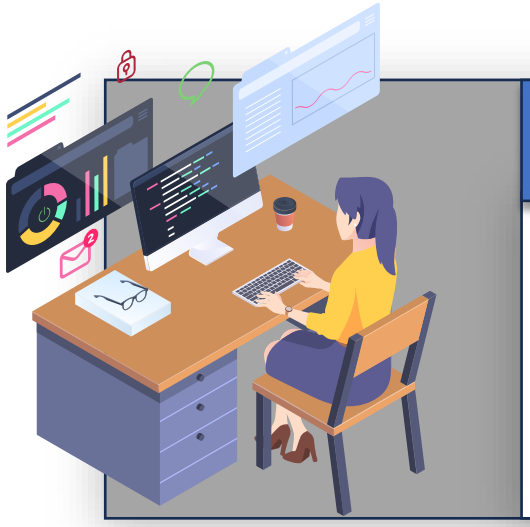
CISSP, CAP, CEH, NSA IAM/IEM, CHFI, CECS, ITIL v3
ICT/Cyber Supply Chain Risk Management (SCRM) Service Element Lead | NASA

Office of the Chief Information Officer (OCIO)
Cybersecurity Service Line (CyS)
240.472.3371 – cell
SIPR Email: kanitra.tyler@nss.sgov.gov
JWICS Email: kanitra.tyler@nasa.ic.gov

Questions?

Self Attestation: In-House / Contracted Service (Out of Scope)

Jira Microsoft Visual Studio Azure Dreamweaver



Attestation Required

Software used for development

Attestation Not Req.

Software developed by or on behalf of NASA

GitLab GitHub AWS Google Cloud PyCharm Professional

NOTE: NPR 7150 should be followed for development within the NASA environment

Self Attestation: Commercial Acquisitions (In Scope)

1 Customer [Commercial IT Request (CITR)]

2 IT Acquisition Dependencies (NF1707 Checks)

3 ICT/C-SCRM (SCRAs)

4 Checks RSAA

5 Commercial Software product with noted presence of attestation & association with NASA in RSAA, or not, added to CAP