National Aeronautics and Space Administration

Secure Software Development Self-Attestation Collaboration Opportunity #2

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

July 24, 2024

www.nasa.gov

Office of the Chief Information Officer

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.”

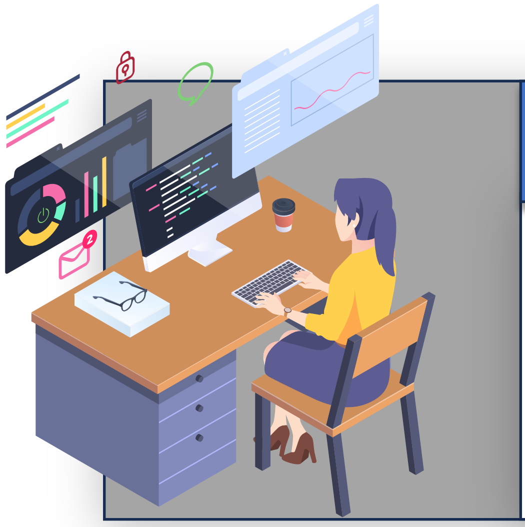
Consistent with these authorities and the directives of EO 14028, each Federal agency is required to comply with the NIST Guidance when using third-party software on the agency’s information systems or otherwise affecting the agency’s information.

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

- Clarification – Software Developed By or on Behalf of NASA & Commercially Acquired
- Navigating CISAs Repository for Attestations and Artifacts (RSAA)
- Question & Answer

Self Attestation: In-House / Contracted Service



Attestation Required

Software used for development

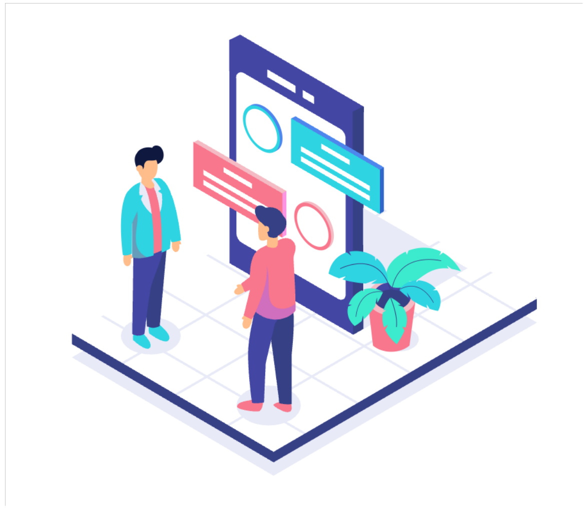
→

Attestation Not Req.

Software developed by or on behalf of NASA

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

Self Attestation: Commercial Acquisitions



1 Customer Commercial IT Request (CITR)

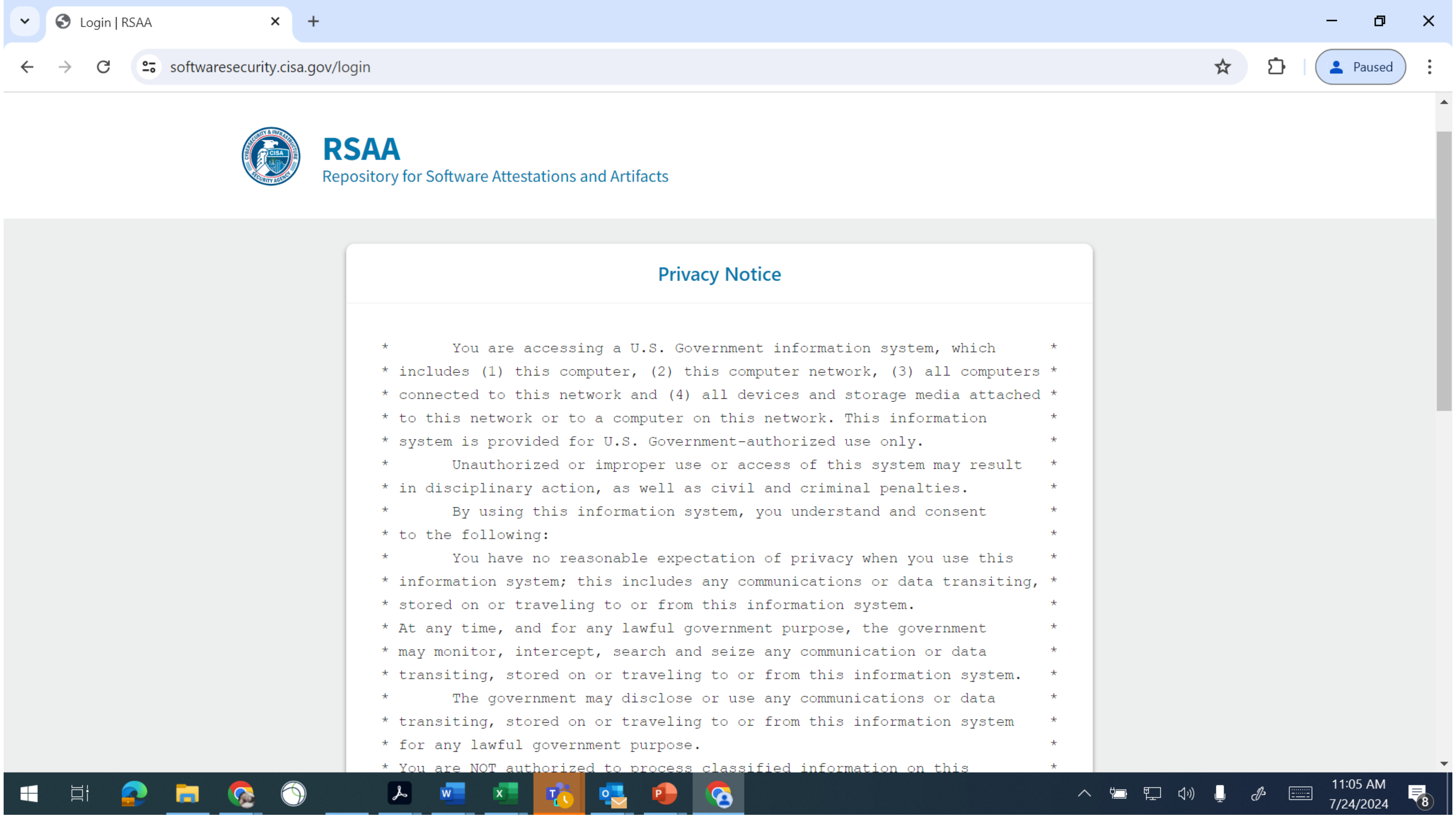
2 IT Acquisition Dependencies (NF1707 Checks)

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

Repository for Software Attestations and Artifacts



RSAA

Repository for Software Attestations and Artifacts

Privacy Notice

```
*       You are accessing a U.S. Government information system, which     *
* includes (1) this computer, (2) this computer network, (3) all computers *
* connected to this network and (4) all devices and storage media attached *
* to this network or to a computer on this network. This information      *
* system is provided for U.S. Government-authorized use only.             *
*       Unauthorized or improper use or access of this system may result  *
* in disciplinary action, as well as civil and criminal penalties.        *
*       By using this information system, you understand and consent      *
* to the following:                                                        *
*       You have no reasonable expectation of privacy when you use this   *
* information system; this includes any communications or data transiting, *
* stored on or traveling to or from this information system.              *
* At any time, and for any lawful government purpose, the government      *
* may monitor, intercept, search and seize any communication or data      *
* transiting, stored on or traveling to or from this information system.  *
*       The government may disclose or use any communications or data     *
* transiting, stored on or traveling to or from this information system   *
* for any lawful government purpose.                                       *
* You are NOT authorized to process classified information on this        *
```

Resources

- RSAA - https://softwaresecurity.cisa.gov/login
- 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

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?

Agenda

- Executive Order 14028 Definition & Identification of **Critical** Software
- Associated OMB Requirements
- Scope
- Timeline for Implementation
- Extensions (cannot attest right now) & NASA’s Process
- Waivers (will never attest) & NASA’s Process
- NASA’s Current Status
- What We Need from You
- Question & Answer

Executive Order 14028, Section 4, Securing the Software Supply Chain

- SCOPE
  - *EO-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.
  - The definition applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software), regardless of operating environment, purchased for, or deployed in, production systems and used for operational purposes.
  - NASA must take action to identify, protect/secure and remove categories of "critical software" from the environment and available contract vehicles . Extensions & Waivers, with exceptional justification, can be requested if products in a critical category of software is required to maintain mission and business essential functions.

Executive Order 14028 – EO-critical software Categories

- ICAM
- Operating systems, hypervisors, container environments
- Web browsers
- Endpoint security
- Network control
- Network protection
- Network monitoring and configuration
- Operational monitoring and analysis
- Remote scanning
- Remote access and configuration management
- Backup/recovery and remote storage

https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory

Identifying NASA-critical software.

- Criticality is defined as a measure of the degree to which an organization depends on the information or information system, and components, including software, contained within, for the success of a mission or of a business function. [Sources: CNSSI 4009-2015, NIST SP 800-60]
- Criticality Categories
  - ✓ Category 1: Critical Functions--Mission-Critical.
  - ✓ Category 2: Essential Functions--Vital.
  - ✓ Category 3: Necessary Functions--Important.
  - ✓ Category 4: Desirable Functions--Minor.
- What Does this Mean to NASA (WDTM2N)?
  - ✓ NASA Standard 2804
  - ✓ NASA High-value Assets (HVAs) and Mission-Essential Functions (MEFs)

OMB Policy

M-22-18: *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*

- “A software producer’s **self-attestation** serves as a ‘conformance statement’ described by the NIST Guidance.”
- “Consistent with the NIST Guidance and by the timelines identified below, agencies are required to obtain a **self-attestation** from the software producer before using the software.”

M-23-16: Update to M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*

- “This memorandum reinforces the requirements established in M-22-18, reaffirms the importance of secure software development practices, and **extends the timelines for agencies to collect attestations from software producers**.”

Scope

TLP:GREEN

Applies to:

- Software developed, or released, after September 14, 2022;
- Software developed prior to September 14, 2022, but modified by a major version change after September 14, 2022; or
- Software code where the producer delivers continuous changes (such as software-as-a-service products or other products using continuous delivery/continuous deployment).

Scope

TLP:GREEN

Does not apply to:

1. Software developed by Federal agencies
   - If there are questions regarding whether software developed by Federal contractors should be considered agency-developed, agency CIOs are required to make that determination on behalf of the agency.
   - Agencies are expected to leverage the NIST Secure Software Development Framework (SSDF) requirements specified in the form.
2. Open-source software that is freely and directly obtained by a Federal Agency
3. Third party components
   - Software producers ARE required to:
     - Maintain trusted source code supply chains
     - Document and minimize use of software products that create undue risk
     - Maintain provenance
     - Software producer employs automated tools or comparable processes that check for security vulnerabilities.
4. Freely obtained and publicly available proprietary software

TLP:GREEN

Timeline for Implementation

Important Deadlines

- March 8, 2024, Form Release
- ~~May 9, 2024, Extensions and waivers deadline for **critical software**~~
- ~~June 8, 2024, **Critical software** attestation collection deadline~~
- August 9, 2024, Extensions and waivers deadline for **all software**
- September 8, 2024, **All software** attestation collection deadline

TLP:GREEN

When a software producer cannot attest…

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 Extensions/POA&Ms

- Software publisher responsibility to submit extension/POA&Ms for software for which the publisher cannot attest to secure software development practice(s) **at this time**
  - ✓ Common Form 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			

TLP:GREEN

When a software producer cannot attest…

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 Waivers

- Software publisher responsibility to submit waivers for software for which the publisher will **never** attest to secure software development practice(s)
  - ✓ Common Form 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

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)			

NASA’s Current Status

- Known software inventory has been collected
- Initiated process to “associate” NASA with available attestations, software records and artifacts in CISAs Repository for Software Attestations and Artifacts (RSAA)
- Mapped “Common Form” requirements to NIST SP800-53 controls, and, identified those that are Agency Common Controls
- Released memo *Update to January 2023 Supplier Documentation Requirements for Software Producers Offering Third-Party Software to NASA for Purchase and/or Use* co-signed by the Assistant Administrator for Procurement and Chief Information Officer
- Initiated weekly Collaboration Opportunities

What we need from you to ensure NASAs success!

- Upload self-attestation and associated artifacts into RSAA.
- Communicate with NASA Software Attestation POCs via Agency-DL-SoftwareAttestation@mail.nasa.gov if there are additional questions or to submit extensions/POA&Ms and waiver requests.

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?

Back-up

NASA’s Extensions/PO&AM Template

As outlined in NASA’s June 2024 memorandum, **Plans of Action & Milestones (POA&Ms)** will be required to document the secure software development (SSD) practice(s) that cannot be attested to **at this time**. At a minimum, the POA&M must document:

i. Common Form practice(s) that the software publisher cannot attest to.
iii. Compensating or mitigating practice(s).
iii. Date the Common Form practice(s) will be implemented.

Please place a 'X' in column A to identify the Common Form Practice and complete additional columns (B - F) with requested information.

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			
	1f	SA-3(1), SA-8, SA-15			
	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)			
	3	SA-3(1), SA-4, SA-8, SA-9, SA-10, SA-10(1), SA-15, SR-3, SR-4, SR-5			
	4	SA-5, SA-9, SA-10, SA-11, SA-11(1), SA-11(4), SA-11(5), SA-11(8), SA-15, SA-15(1), SA-15(7), SA-15(10), SA-15(11), SR-3, SR-4, SR-4(3), SR-4(4), SR-9			

NASA's Waiver Template

If a software publisher will never be able to attest to Common Form practice(s), a **waiver** request must be submitted. At a minimum, the waiver request must document:

i. Common Form practice(s) that the software publisher will never be able to attest to.
ii. Compensating or mitigating practice(s).
iii. Risk Mitigation Strategy(ies)

Please place a **'X'** in column A to identify the Common Form Practice and complete additional columns (B - F) with requested information.

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]**
	1a, b, c, d & f	SA-3(1), SA-8, SA-15			
	1f	SA-3(1), SA-8, SA-15			
	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)			
	3	SA-3(1), SA-4, SA-8, SA-9, SA-10, SA-10(1), SA-15, SR-3, SR-4, SR-5			
	4	SA-5, SA-9, SA-10, SA-11, SA-11(1), SA-11(4), SA-11(5), SA-11(8), SA-15, SA-15(1), SA-15(7), SA-15(10), SA-15(11), SR-3, SR-4, SR-4(3), SR-4(4), SR-9			