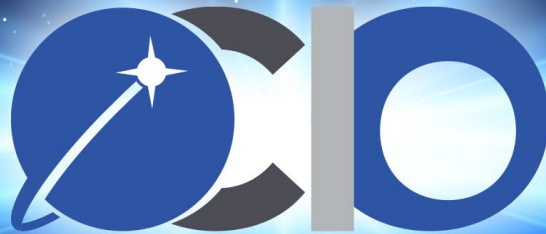




# Secure Software Development Self-Attestation Collaboration Opportunity #3



Kanitra Tyler, ICT/C-SCRM Service Element Lead  
Kay Twitchell, Deputy Software License & Asset Manager  
July 31, 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](mailto: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.



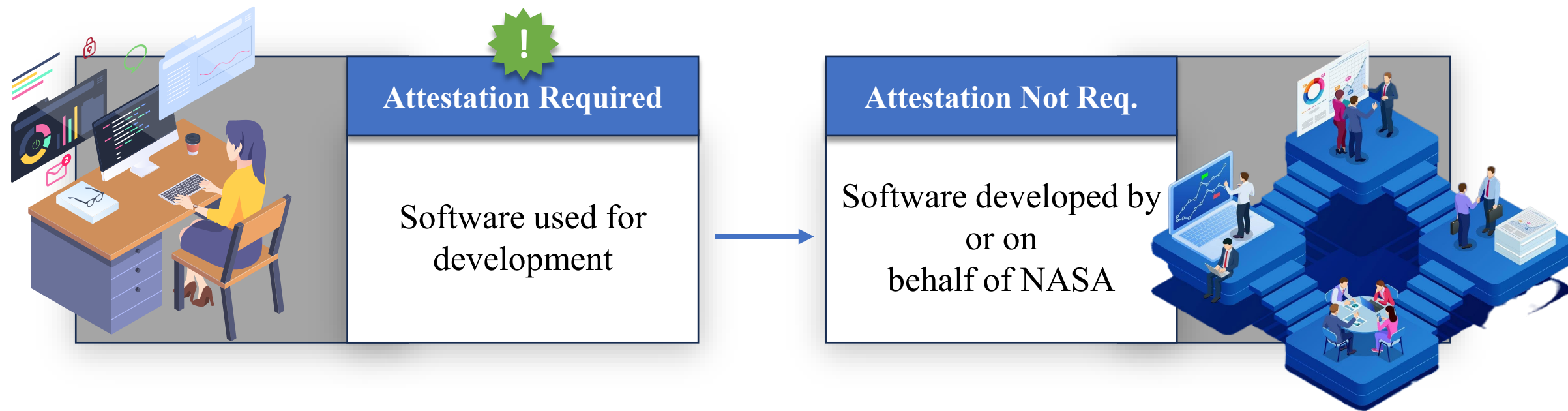
# Agenda

- Clarification – Software Developed By or on Behalf of NASA & Commercially Acquired
- Navigating [CISAs Repository for Attestations and Artifacts \(RSAA\)](#), a Software Publisher's Perspective
- Attestation Alternatives
- Question & Answer



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

Jira Microsoft Visual Studio Azure Dreamweaver



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





# Repository for Software Attestations and Artifacts

Browser window: Login | RSAA  
Address bar: softwaresecurity.cisa.gov/login

 **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 \*  
\*

Taskbar: Windows, Edge, File Explorer, Chrome, Task View, Word, Excel, Teams, Outlook, PowerPoint, Edge, System tray: 11:05 AM, 7/24/2024, 8 notifications



## **BUSINESS CYBER GUARDIAN™ :**

A Software Engineering Company dedicated to software supply chain cyber-risk detection solutions for companies, and Active Member of the CISA ICT\_SCRM Task Force Software Assurance Workgroup

# **Attestation Collection: A Software Publishers Perspective**

Dick Brooks, Lead Software Engineer

[dick@businesscyberguardian.com](mailto:dick@businesscyberguardian.com)



# Agenda

- BCG background
- CISA's Secure Software Attestation Form Expectations and RSAA Portal
- Guidance and Lessons Learned



# BCG Background

- Software Engineering Company in Westfield, MA providing ICT\_SCRM products and services to illuminate cyber-risks and verify products against the “CISA Common Form” requirements for both producers and consumers of software products
- Contributor to CISA Software Acquisition Guide
- Information and Communications Technology Supply Chain Risk Management (SCRM) Task Force Member
- Critical Manufacturing Sector Coordinating Council (CMSCC) Information Technology Subject Matter Expert Contributor
- Adviser to Healthcare Sector Coordinating Council
- What does BCG do?



# BCG Products and Services

- Software Assurance Guardian Point Man (SAG-PM™)
  - Cyber-risk illumination tool to verify products for NIST Guidance in OMB-M-22-18 and the CISA Buyers Guide recommendations
    - SEC Cybersecurity Disclosure Regulations (17 CFR 229.106)
    - FDA Vulnerability Disclosure Reporting for MDM
    - Executive Order 14028 and OMB M-22-18 compliance
    - GSA SCRIPTS RFQ BPA “ready”
- Software Assurance Guardian Community Trust Registry (SAG-CTR™)
  - Cloud based verification and cyber-risk reporting service using SAG-PM
  - CISA Common Form verification services
  - Enables parties to register trust in software products and share findings with other agencies
    - Supports Internet Engineering Task Force (IETF) Supply Chain Integrity, Transparency and Trust (SCITT) concept listing trusted products (Cloud Service, running on AWS)




# CISA's Secure Software Attestation Form

- Authority: Governing laws including 44 U.S.C. § 3554, E.O.14028, and OMB Memorandum M-22-18
- Conditions for Self-Attestation: Software development date or significant version changes after specified dates
- Exclusions from Self-Attestation: Federal agency-developed software, freely obtained/open-source software, and certain third-party components
- Submission Instructions: Online form via provided URL or PDF submission with specific naming convention
- Form Completion: Requires description of software and producer info; CEO or designee signature necessary
- Third-Party Assessment Option: Performed by a certified or approved Third Party Assessor Organization



# CISA's Forthcoming Buyer's Guide

- 
- Key artifact with description of detailed Secure by Design requirements
  - A “how-to” manual for Secure by Design
  - Identifies management of required information to customers
    - Organize, prepare and communicate
  - IETF SCITT Vendor Response Form
    - Enables software consumers to retrieve information from a known trusted source
    - Supports US Cyber Trust Mark
    - Demo'd at IETF 117 Hackathon



## **Cybersecurity and Infrastructure Security Agency (CISA) Repository for Software Attestations and Artifacts (RSAA) User Guide**

---

Publication: March 2024  
Cybersecurity and Infrastructure Security Agency

<https://www.cisa.gov/resources-tools/resources/repository-software-attestations-and-artifacts-rsaa-user-guide>



# RSAA

Repository for Software Attestations and Artifacts



## RSAA

Repository for Software Attestations and Artifacts

Login to the Repository for Software Attestations and Artifacts

Log in to RSAA

OR

Request an Account

If you have already been approved for access to RSAA, please proceed to login. Otherwise, if you have a need to access this system in an official capacity, please request an account.



Stronger security with  
Google Authenticator

Get verification codes for all your accounts using  
2-Step Verification

Get started

<https://softwaresecurity.cisa.gov/login>



# RSAA

Repository for Software Attestations and Artifacts

User: **DICK BROOKS** | Role: **Software Producer** | Company: **Reliable Energy Analytic** | [Logout](#)

[Software Records](#) | [Artifacts](#) | [Attestations](#)

Home / [Software](#)

## Software Records

[Create Record](#)

Search software records by software name, contact, etc.



Filter by Agency



Filter by Status



Sort by Software Name



[Reset Search](#)

[Software Assurance Guardian Point Man \(SAG-PM\), 1.2.2-1.2.2](#)

[Status](#)



By: [Reliable Energy Analytic](#)

Created on 04/01/2024, 08:27:15 AM EDT

<https://softwaresecurity.cisa.gov/login>





# RSAA

Repository for Software Attestations and Artifacts



## Software Record

Agency View

National Aeronautics and Space Administration

Software Assurance Guardian Point Man (SAG-PM), 1.2.2-1.2.2 [Released 12/15/2023]



### SOFTWARE PRODUCER

#### Reliable Energy Analytic

23 Linda Dr, Westfield, MA 01085, USA

Website: <https://reliableenergyanalytics.com/>

### CONTACT


#### Dick Brooks

Co-Founder

Tel: *No Data*

Email: [dick@reliableenergyanalytics.com](mailto:dick@reliableenergyanalytics.com)

### AGENCY STATUSES

Agency	Last Updated By	Updated On	Status
 No data			



# RSAA

Repository for Software Attestations and Artifacts



## Attestations

New Attestation

(SAG-PM) V 1.2.2 Secure Software Attestation Form - Requires POA&M

accepted



Software Producer: Reliable Energy Analytic  
Attested By: Uploaded Attestation

Created by Dick Brooks on 04/03/2024, 08:20:31 AM EDT

< 1 > 25 / page

## Artifacts

Upload Artifact

2024-04-13 POA&M for NASA using DoD format in Excel

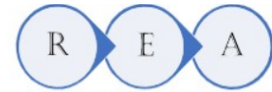


Description: No data  
Type: Plan of Action and Milestones

File: [SAG-PM-V1-2-2-POAM-2024-0408.xls](#) accepted

Created by Dick Brooks on 04/13/2024, 08:50:50 AM EDT

# SAG-CTR Demonstration: Sharing Results



RELIABLE ENERGY ANALYTICS LLC

## Welcome to SAG-CTR (TM)

DISCLAIMER: Reliable Energy Analytics LLC (REA) makes no warranty or guarantees as to the accuracy or completeness of the information available on this site. All information has been freely provided by trusted parties solely as a means to share information about their risk assessment experiences with digital products without any claim or guarantee as to their fitness of purpose or freedom from defects or vulnerabilities that could potentially cause harm. Use the information in SAG-CTR at your own risk.

— Reliable Energy Analytics LLC (REA) REA Officers and Directors

Choose a Product Category:  Choose a Label Type:

[Get Products](#)

Trusted Products List

No Product Found

© 2018-2024 Copyright:Reliable Energy Analytics LLC (REA),\_Version: 2024-03-29

SAG-CTR APIs are available for easy integration into other dashboard products and websites, such as app stores:


- <https://softwareassuranceguardian.com/SAGCTR/>
- [https://softwareassuranceguardian.com/SAGCTR\\_inquiry/getProductCategories](https://softwareassuranceguardian.com/SAGCTR_inquiry/getProductCategories)
- [https://softwareassuranceguardian.com/SAGCTR\\_inquiry/getLabelTypes](https://softwareassuranceguardian.com/SAGCTR_inquiry/getLabelTypes)
- [https://softwareassuranceguardian.com/SAGCTR\\_inquiry/getSAGScore?FileHash=48E0EEB4C538BCD65514D68DDA5E1B41BE9F38AAB3A9B4108F056A27BE1F379A](https://softwareassuranceguardian.com/SAGCTR_inquiry/getSAGScore?FileHash=48E0EEB4C538BCD65514D68DDA5E1B41BE9F38AAB3A9B4108F056A27BE1F379A)

# Lessons Learned

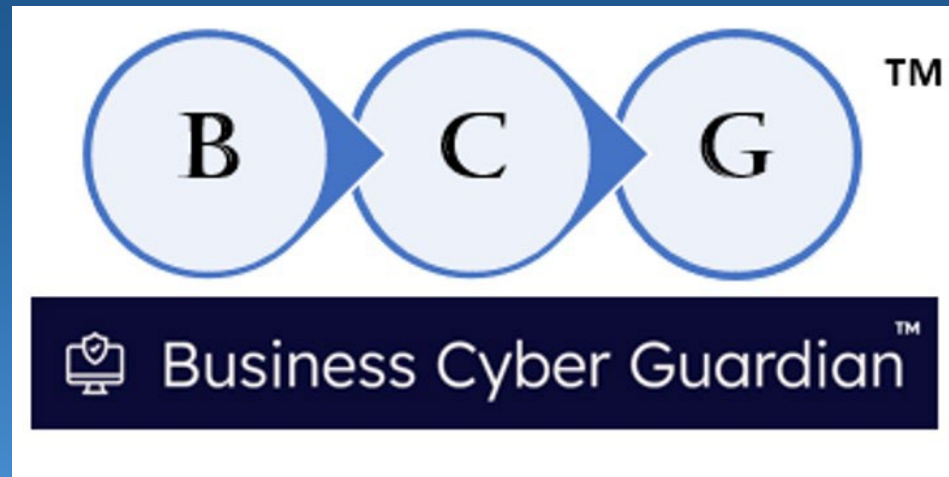
- Software Suppliers need to apply for an RSAA account; can take a few days to complete
  - An authenticator app is needed for MFA (REA uses the Google App)
- Only one artifact is required: A Fully Executed CISA Secure Software Attestation Form
- Attestation form can represent a single product or an entire product line; REA submitted a “product attestation”
- Agencies may also request other artifacts, such as an SBOM and Vulnerability Disclosure Report (VDR) **see Buyers Guide for details**
- Software Suppliers should prepare by organizing all of the artifacts using a Vendor Response Form (VRF document) – not required, but useful for keeping a “RSAA submission package organized”. BCG submitted its VRF package as an artifact in RSAA.
- BCG anticipated having to supply all of the required and optional artifacts and prepared by uploading all artifacts to RSAA as a package
  - Artifact uploads can be slow to process – over a minute to accept/reject



# Lessons Learned

- 
- Artifacts need to be “Attached” to an Attestation (separate step)
  - Attestations need to be “Attached” to a software record (separate step)
  - Attestations need to be “Associated” with an Agency/Department in RSAA
  - There are some open questions about using RSAA to indicate that an attestation requires a POA&M (**will be addressed in Buyers Guide FAQ**)
  - Recommend that Software Suppliers use the Buyers Guide Spreadsheet for the best chance at “passing the attestation test”, based on the Buyers Guide materials.
  - Consider the benefits of sharing RSAA processing results with other agencies using a “Trust Registry”, like IETF SCITT
  - It’s in a suppliers best interest to provide information up front, in the RSAA portal, to avoid back-forth on items the “Common Form” doesn’t address, like foreign ownership and influence (FOCI)

# Questions?



Thank You

Dick Brooks

[dick@businesscyberguardian.com](mailto:dick@businesscyberguardian.com)



# Attestation Alternatives

- FedRAMP Third Party Assessment Organization (3PAO)
- Certification / Authorization Types
  - ✓ FedRAMP Authorization
  - ✓ National Institute of Standard & Technology (NIST) – 800-53 or 800-171
  - ✓ Capability Maturity Model Integration (CMMI)



# Resources

- NASA Knowledge Center (internal) – [https://nasa.sharepoint.com/sites/ictscrm/SitePages/SCRM-Knowledge-Center\(1\).aspx](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](https://www.cisa.gov/sites/default/files/2024-03/CISA_RSAA_User_Guide_18_March_2024.pdf)
- 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](mailto:kanitra.tyler@nss.sgov.gov)

JWICS Email: [kanitra.tyler@nasa.ic.gov](mailto:kanitra.tyler@nasa.ic.gov)

## Questions?