Software & Supply Chain Assurance for GSA IT

Office of the Chief Information Security Officer

5/31/23

Presented by: Armando Quintana Nieves and William Salamon
Meet the team - GSA IT, Office of the CISO

Armando Quintana Nieves
Director, Security Operations Division (ISO)

William Salamon
Director, ICAM Shared Services Division (ISI)
Agenda

01 Overview

02 C-SCRM Program

03 Enterprise Vulnerability Management Program
Who are we?

- We work for the GSA Office of the CISO, within GSA’s CIO office leading programs for:
  - Cyber supply chain risk management for the systems that we manage or oversee
  - Enterprise Vulnerability Management for identifying and prioritizing known vulnerabilities
  - DevSecOps where we work with development teams to integrate security best practices into their development pipelines
- Our organization is responsible for securing the GSA enterprise and systems and is distinct from the government-wide services provided by the Federal Acquisition Service or the Office of Government-wide Policy.
- GSA provides solutions used by other agencies and by vendors that want to work with the government. This is done via solutions that are custom-developed by GSA, supported by COTS products, and also SaaS vendors. Each of these software types pose risks that are managed in different ways.
C-SCRM Program
Foundational Activities

- **POLICY**
  - C-SCRM requirements in GSA acquisitions
  - Established Bug Bounty Program
  - Created Vulnerability Disclosure Policy

- **PROCEDURE**
  - Red Team assessments of OT/IoT networks
  - Device Discovery and Profiling w/Network Access Controls

- **PROCESS**
  - Securing GSA usage of drones (UAS)
  - Einstein E1, E2, E3a, FireEye and 24x7x365 GSA SOC
  - IT Standards review/approval for software to include supplier risk
  - Address C-SCRM requirements identified in NIST SP 800-53 Rev 5
C-SCRM Program: Goals and Objectives

Synergize

GSA OCISO Cyber Security and Supply Chain Risk Management expertise

Assess

GSA IT’s Cyber risk from 3rd party suppliers and their products prior to a major business award

Continuously Monitor

Assess risks from awarded IT products and services

Advise

Establish C-SCRM governing policies for GSA IT acquisitions and systems (on-prem + vendor)
Critical IT Supplier List Methodology

**Hardware & Software Assets**
- Any contracted SW or HW which connects to GSA network (Includes buildings devices)
- Device and software list compiled and suppliers identified for risk analysis

**Integrators**
- Contractor support for IT development and other technical services

**FISMA Systems**
- Ultimate suppliers for FISMA High and Moderate systems
- Results are recorded for continuous monitoring through VRA tools

**Financial Risk**
- Financial Exposure (overall cost can indicate criticality)
C-SCRM Program: Component Breakdowns

Pre-Award
Assessment of suppliers and their products prior to award

- Analysis focused on possible supplier risks
- Utilize Supplier Illumination tools and other OSINT capabilities

Post-Award
Activities relating to supplier continuous monitoring and auditing

- Hardware Device Component Testing
- Use third party supplier illumination tools & SME analysis
- Automated alerting for cyber supply chain events

Ongoing C-SCRM Support
Maintain the operational effectiveness of the program

- NIST SP 800-53 Rev 5 Supply Chain common controls
- Periodic updates to GSA Critical IT Suppliers

Respond to Cyber Supply Chain events and incidents
The Cyber Executive Order 14028 has resulted in substantial changes in how the government buys software:

- The Cyber EO tasked NTIA to define ‘minimum elements’ for a Software Bill of Materials (SBOM).
- NIST updated NIST SP 800-218 and OMB issued M-22-18 to require vendor attestations to software security best practices to include provenance (e.g. SBOMs).
- The scope for a mandate for SBOMs for software the government purchases is still forthcoming.

What will we do with these SBOMs once we have them?

- One of the best use cases for having SBOMs came during the response Log4j.
- What was a difficult process in data calls to internal teams and external vendors could be immediately available the next time something happens if we have SBOMs and a view of the software components for software in our systems.
Enterprise Vulnerability Management Program
Current Vulnerability Management Program State

The GSA program is made up of a variety of resources to determine the risk posture of the environment, including the following:

- CyHy Report
- Bug Bounty / Vulnerability Disclosure Program
- OS & Database Scanning
- Web Application Scanning
- Containers Scanning
- Multi-Cloud Environment Scanning

- KEVs Reports (BOD-22-01)
- Critical/High Vulnerability (BOD-19-02)
- Penetration Testing / Red Team Results
- Mobile Vulnerability - Lookout for Work
- SAST w/ SCA (coming)
- AWARE Report (Future State)
GSA Asset/Software Discovery Solution

- GSA uses a semi-active discovery solution
- Uses a variety of methods:
  - Agents (provide additional contextual information)
    - Appliances installed in each region & data center with connections to core switches
    - Passive listening to network via span ports
    - Connection to wireless APs
Vulnerability Enumeration - OS and Database

Faster enumeration means more accurate results of threat risk

Agent-based vulnerability enumeration every 72 hrs
Active scans are run against all hosts every 7 days

Combination Agent / Active Vulnerability Enumeration

30,000+ devices

15,000+ Workstations across CONUS

Mobile Vulnerability 11,000+ Android/iOS
Vulnerability Enumeration - Web (Internal / External)

Faster enumeration means more accurate results of threat risk

2,500+ URL (Internal/External)

Challenges

- Monthly Unauthenticated Scan
- Annually Authenticated Scan
  - continuous integration/continuous deployment (CI/CD) pipelines

- Manual Authentication Scan
- API Scan (Initial)
Container Vulnerability Management

1. GSA-managed & built
   - Less risk
   - Faster patching

2. Vendor-provided
   - Moderate risk
   - Hold vendor accountable for patching

3. Open source
   - High risk
   - Patched by Open Source Community

Challenges:

1. Vendor recommends application/system teams not to alter vendor container images.
2. Multiple (different) teams are working on fixing vulnerabilities in the same images.
3. Deployment CVE management becomes more difficult than traditional OS, due to the nature of container images.
GSA Prioritization Considerations

- More frequent scanning helps technical team know if patches are remediate

<table>
<thead>
<tr>
<th>Devices with Public Presence</th>
<th>Others</th>
<th>Known Exploitable Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical: 15 days</td>
<td>Critical: 30 days</td>
<td>Within 14 days</td>
</tr>
<tr>
<td>High: 30 days</td>
<td>High: 30 days</td>
<td></td>
</tr>
<tr>
<td>Moderate: 90 days</td>
<td>Moderate: 90 days</td>
<td></td>
</tr>
<tr>
<td>Low: 180 days</td>
<td>Low: 180 days</td>
<td></td>
</tr>
</tbody>
</table>
Software Security for GSA IT

Supply Chain
- CI/CD pipeline
- Static code scanning
- Dynamic code scanning
- Dependencies / Software Composition Analysis
- DevSecOps

Secure Development
- Understand how code is maintained from start to finished
- Response to critical component vulnerabilities (e.g. log4j)

Vulnerability Management
- Understand vulnerabilities of underlying systems & apps
  - OS/Database/Apps
  - VDP/BB
  - DAST/IAST/RASP

Software Types
- COTS/GOTS/Open Source

Who maintains code
- Vendor/Open Source Community

Tools
- SBOMs
- Vendor C-SCRM assessments
Thank you!

Armando Quintana Nieves  
Director, Security Operations Division  
GSA IT, Office of the CISO  
armando.quintananieves@gsa.gov

William Salamon  
Director, ICAM Shared Services Division  
GSA IT, Office of the CISO  
william.salamon@gsa.gov