This position paper is being sent on behalf of Copado in response to the National Telecommunications and Information Administration (NTIA) Request for Public Comment on "Software Bill of Materials (SBOM) Elements and Considerations" to help NTIA fulfill Executive Order (EO) on Improving the Cybersecurity of the Federal Government (14028).

Copado appreciates the honor of recommending best practices in regards to building Software Bill of Materials within Infrastructure as a Service, Platform as a Service, and Software as a Service organizations.

The purpose of this paper is to address the EO request for automated, vendor-agnostic, and machine speed requirements to respond to cyber threats more rapidly and create more resilient software for the nation.

The Software Bill of Materials (SBOM) will be a great advantage for national software resilience when established as a best practice for secure software development in cloud ecosystems. Software as a Service, Platform as a Service, or Infrastructure as a Service organizations are extremely large and complex software environments. Having a standard format and best practices for SBOM will allow industry to build and commercialize tools to create efficiency in the capturing and maintaining of all software assets. This capability will help cross-functional teams such as cybersecurity, IT operations, software development, and legal to operate more efficiently, building more resilient software for our nation.

SBOMs will be a critical best practice for building transparent software platforms that are easier to defend by giving visibility to the organizations responsible for that defense.

That visibility of all software utilized in the building of cloud software is important to being able to respond to security threats quickly, being able to strengthen capabilities in assessing risk, and allowing transparency during investigation phases post security incident. Not only are there significant security challenges that SBOM assists with, but proper SBOM implementation can also be beneficial to the organization in a variety of ways that are outlined below.

This cannot be accomplished unless there is a national standard for SBOM that allows industry to build standards-based solutions for the management of SBOM.

Copado and is acquired company New Context are participating in SBOM working groups and have been working to create implementation strategies for ourselves and our customers around SBOM. The recommendations in this document are part of the strategies that we will be deploying, or have been depoying, for ourselves and our customers.

Foundation of DevOps/DevSecOps

SBOM is machine-readable format to support large software environments that are too complex for a humans to parse. That is why it is critical to ensure DevOps build environments are set up appropriately to create SBOMs automatically as part of the software development life cycle. This automation reduces the burden of maintaining the SBOM while allowing the creation of verbose

software component lists that can be read and parsed easily by other computer systems. DevOps will be important to keep the cost of updating and maintaining SBOM low, so that the industry will be more willing to adopt.

Four specific benefits that SBOM can bring to cloud systems:

- CyberSecurity: SBOM adoption by cybersecurity organizations allows for rapid ability to address threats as they come in in real time and a faster mean time to incident resolution.
    - Incident Response
        - SBOM feeds integrated into SOC operations through the SIEM
        - SBOM in combination with STIX opens a great ability for threat intel correlation and matching
        - SBOM and OpenC2 allow for rapid machine response such as automated patching or software workarounds
        - SBOM and CACAO gives the capability for standard playbooks to respond to software-related security incidents
    - Vulnerability assessment
        - SBOM, when fully implemented at the highest depth, ties aggregate products back to the complete tree of components, which can be used for vulnerability management and remediation
        - Provides a common integration point for other systems, as a standard, tying SBOM to other systems such as threat intel platforms, security incident and event management (SIEM) systems, and vulnerability assessment platforms
        - Increased visibility into component vulnerabilities enables proactive response and threat mitigation
    - Forensics
        - Similar to how log files help organizations analyze security incidents, SBOM databases can help identify the root causes of incidents. SBOMs will be useful in giving insights into tactics, techniques and practices of intruders
- IT Operations: SBOM adoption by Operational IT groups holds value, provided the information is maintained in an automated and vendor-agnostic manner, by providing machine-speed answers to the operational concerns listed below.
    - Operational compliance and consistency
        - Attribution of components in running systems - via cryptographic signature or other well-known format
        - Provide a standardized point of reference for infrastructure compliance and assurance auditing
        - Assurance that what is in production is what we expect
- Software Development: SBOM adoption by software development groups enhances the ability of software publishing organizations to understand the entirety of their

development ecosystem by documenting the dependencies introduced as a product or service evolves.
    - Software Supply Chain
        - Enhances trust relationships with vendors by providing deep views into component composition early in the software lifecycle, where risk management and mitigation yield the highest return on investment
        - Provides a machine-readable framework for documenting the entire supply chain related to a particular product or service
    - Vendor Selection
        - Improves decision-making ability when selecting third-party components based upon a common set of descriptive information
- Legal: As an ancillary benefit to implementing SBOM, transparency and visibility into software licensing IP can help legal teams assess ownership and IP controls more efficiently in an automated fashion.
    - Licensing/IP reviews
        - Integration point for legal inventory of a product
        - Provides a Single Source of Truth - surfacing legal/ip/compliance in a standardized way to enable rapid auditing and compliance checking.
        - Reduced risk due to increased visibility to component legal/licensing issues

Integration Recommendations

To take advantage of automated, vendor-agnostic and machine speed capabilities, SBOM must be integrated into enterprise software systems. These integrations will enable the data of SBOM to be used with command and control (C2) systems.

- Security Information and Event Management (SIEM)
    - Vulnerable Component Detection
        - Service or Application Launcher sends SBOM to SIEM on activation
        - SIEM notifies SOC when insecure or disallowed components are used
- Security Operations Center (SOC)
    - Critical Vulnerability Exploit (CVE) Response
        - When notified of a CVE, SOC can search the Software Asset System to determine which applications and services are vulnerable
        - SOC contacts application/service owners to expedite remediation
        - STIX, OpenC2, CACAO, threat hunting
- Software Asset Systems
    - Dependency Management
        - SBOM enumerates dependencies of deployed applications and services
        - Upstream changes and updates are mapped to managed assets to prioritize updates and forecast disruptions
- Legal and IP Asset System
    - Software License Management
        - SBOM includes license information for dependencies

        - Legal teams review licenses to ensure compliance with internal licensing policies
        - License changes are associated with managed components to determine required actions
    - IP Identification
        - When identifying intellectual property, SBOM clearly delineates dependencies from additions
        - Custom software is reviewed by IP teams for protection or monetization

SaaS, IaaS, and PaaS - On Prem Deployments
Almost all large and successful cloud environments end up having large customers require an onsite deployment. These customers tend to be financial, government, or other highly regulated organizations. Those on-site deployments in the highly regulated industry will have more rigorous requirements around SBOM. Today, vendors are already requiring software makers to be more transparent about the software they deliver. By implementing SBOM as part of standard software development best practices across all industries, it will streamline an organization's ability to commercialize their software in highly regulated environments.

In Summary
Implementation of SBOMs will become a leading part of cyber defenses as they provide transparency for all software assets, components, and dependencies included in the software supply chain including cloud ecosystems. Ensuring that SBOMs are automated, vendor-agnostic, and machine-speed will allow for integration across enterprise systems to support critical functions. A component of this transparency is the ability to identify and manage risk at scale. With effective risk management, an asset owner is able to reduce their attack surface and defend critical security and business systems. Not only does this have impacts on health and safety, but the added bonus of increased cost savings and efficiency. An SBOM standard will build on top of several related efforts already occurring within security communities to bring together the best practices to strengthen the defenses of our nation’s most critical assets.

Contact Information:
Daniel Riedel
SVP of Strategic Services
Copado
DRiedel@copado.com
415-264-1997
Contributors: Justin Dossey, Kelly Cullinane, Christian Hunt, Steve Kluth, Kevin Chan