Ms. Laurie Locascio, Ph.D.
Under Secretary for Standards and Technology
Department of Commerce
1401 Constitution Ave. NW
Washington, DC 20230

RE: Notice and Request for Information - Docket Number: 220210-0045

Comments from Copado, Inc.

Copado, Inc. (“we", “us”, or “Copado”) appreciates the opportunity to submit comments in response to the National Institute of Standards and Technology’s Request for Information [Docket No. 220210-0045] on *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.*

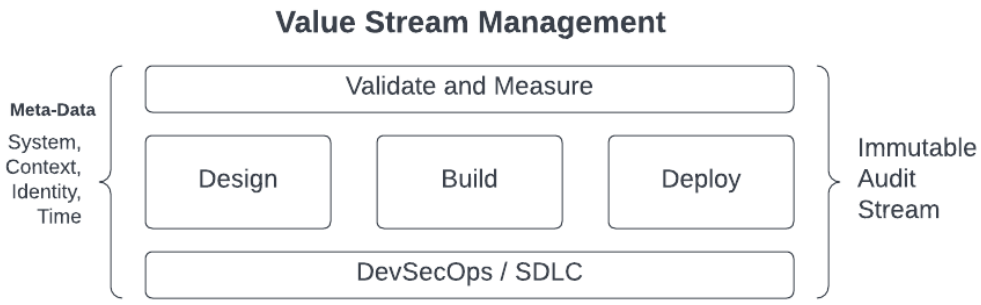
About Copado
Copado is the first DevOps platform built for the low-code SaaS world. We are redefining how to achieve success on the Salesforce platform with a data-driven approach to delivering faster, higher quality releases and improving trust across customer transformation projects. Originally designed for Salesforce, Copado has grown to support a growing number of cloud environments.

Copado & Cybersecurity
Copado is home to a proven world-class security research team. Our security experts have testified before the Senate, helped on Executive order working groups for software supply chain assurance and for the last 7 years contributed to global cybersecurity standards. Currently Copado teams work on significant critical infrastructure security challenges with partners in the US Government, academia, private sector companies, international standards bodies, and more.. Copado is at the leading edge of the evolving policy and standards landscape to include participation in NIST working groups on Executive Order 14028: Improving the Nation’s Cybersecurity via Enhancing Software Supply Chain Security.

Copado understands that defenders cannot protect something that they cannot see. This is supported in similar statements made by White House Officials and industry experts. When something is not seen, or its context is not understood, there is zero chance that meaningful security controls can be in place. Together with other common security best practices, Copado proposes applying value stream mapping and management practices to an enterprise to lead to greater security in the cyber supply chain in the form of forensics, observability, and auditability.

Traditional DevSecOps is a powerful concept for software resiliency, but it is a highly fractured market and is still being applied with varying levels of expertise and discipline. These tools often tax businesses and are implemented in silos. In order to have comprehensive success within an enterprise, businesses must change how they approach the challenge. This is where the adoption of value stream management, and its subset of value stream mapping, can help assist business functions as well as provide cybersecurity and forensics expertise.

A well implemented value stream mapping practice where the data is captured into an immutable repository will capture parts of the enterprise that are traditionally not monitored. This practice will look at end to end behaviors of the Software Development Life Cycle (SDLC) and examine all steps required to release software into production. Value stream mapping will look at traditional events, but will also look at new events, such as system design changes and process improvements or modifications, that are relevant to an organization to add additional context to the forensic process for post incident discovery. This context can be used for understanding motivation, informing root cause analysis, and providing enhanced context in a development environment.



Value stream flow in a SDLC environment

Given the current state of the cybersecurity industry, it is becoming increasingly apparent that one “system of record” in an enterprise is not sufficient, especially for post-incident analysis and forensics. If well implemented, value stream mapping will bring together disparate information from across verticals in an enterprise to create a lattice of assurance that will make it less likely that an adversary can tamper with data to hide their tracks. In more advanced applications, Copado sees a pathway for value stream mapping to have impact on areas such as enhanced behavioral detection.

Secure Software Development Framework (SSDF) Supports Value Stream Mapping

Copado commends NIST for its inclusion of value stream mapping as an industry recommendation for software auditability in the recently approved Secure Software Development Framework (SSDF). The establishment of value stream mapping as a best-practice for the mitigation of risk in software vulnerability management will help companies save time and money when responding to a cyber incident.The auditability benefits of value stream mapping will provide another viewpoint in the full SDLC that will capture events with enhanced context. Traditionally, the deployment phase of the SDLC is the focus, but value stream mapping allows for a deeper look at the planning and design phases as it can forensically look at motivation, root cause, and more in context to the development environment.

What is Value Stream Mapping and Management and Why Use It?

Value stream management has been around for decades, originally gaining popularity in manufacturing physical goods more efficiently and consistently in the first half of the 20th century. Value stream mapping is a subset of Value Stream Management and breaks down process flows, often depicted in visual flowchart format, and examines critical steps and quantifies time and value at each stage. Value stream mapping is then an input to value stream management which is the overall framework for executing the strategy uncovered in the mapping process. When done correctly, this process identifies and remediates inefficiencies, delays, and bottlenecks to transform an organization's business practices. This practice is cross-functional and pulls in many parts of an organization to combine areas where responsibility, authority, budget, and more all come together. Value stream mapping is being adopted at an increasingly greater rate by organizations as it has positive impacts on business functions and finances. Gartner estimated that by 2023, 70% of all organizations will use Value Stream Management.[1] Copado's approach to layer in cybersecurity applicability will expand on the positive impacts.

Value stream mapping tools gather event data from each segment and process in the SDLC. The more accurate and specific the event data, the better the tool will be able to help organizations calculate value and identify blockers in their development process. Copado proposes incorporating specific information with each event to allow for forensics to 'piggyback' on standard value stream mapping theories. Each **event** should also have **time** and **identity** associated with it. The complete record of data + time+ identity will create visibility and observability in an immutable ledger for auditability. This will amplify the ability to run post-incident forensics and establish attribution of bad actors.

[1] https://www.forbes.com/sites/forbesbusinesscouncil/2022/01/06/value-stream-management-the-new-prescription-for-better-roi/?sh=42c880f74b55

A well executed value stream mapping program in software can increase transparency, establish the identity of an information source, and provide for robust forensic analysis. Value stream management concepts focus holistically on the business, bringing in stakeholders across verticals into the security process. As demonstrated by the graphic below, several components across an enterprise can be pulled into a value stream mapping program to maximize impact. Currently, the software development and delivery process is greatly diffused and involves multiple languages, tools, and teams. This creates delays and potentially inhibits the identity of information sources. Value stream management creates connections between all events in a given environment. It maps the linear movements between data, manual processes and handoffs, and operational aspects of a system to provide a deeper understanding of that environment.

Source: Gartner 730782C[2]

Implementing Value Stream Mapping

Implementing value stream management allows the system itself to provide information as to its current operational state. This information can be used in numerous ways, not limited to improving efficiency, reducing costs and quality issues, increasing resiliency and providing enormous benefit in the area of information security. Utilizing this data can help the system become more secure and provide invaluable forensic evidence in the aftermath of an incident. When forensics are the focus, the data will tell a slightly different story.

2 https://blogs.gartner.com/manjunath-bhat/2020/10/02/the-future-of-devops-toolchains-is-already-here-its-just-not-evenly-distributed/

Gathering & Collecting Data

All types of data should be collected, and where possible, using existing systems and infrastructure. Having multiple "systems of record" allows for greater resiliency, and leveraging existing infrastructure -- as opposed to centralizing all data collection -- has many benefits. Examples of events could be one or multiple actions and include: logging systems, access control systems, debugging logs, system and server monitoring tools, software bill of materials, and CI/CD pipeline events. Other relevant data can be collected by incorporating event gathering at every stage of the system development life cycle.

Leveraging existing systems that already collects events across specific domains, such as a production logging server, or a physical security system tracking ingress and egress from an office, and interfacing those systems in such a way that events can be correlated provides a powerful tool for improving and maintaining systems.

Individual events should be time-stamped and digitally signed. This allows the source of the event to be identified and the time the event occured to be recorded, and the entire event to be tamper-resistant. Any change to the contents of the event will invalidate the cryptographic signature or hash. Ultimately, these events could be stored in an immutable ledger. This provides an easy mechanism to audit various aspects of a process, procedure, or system as every event is recorded.

The process of identifying and collecting observables at various stages of the SDLC goes a long way towards helping to improve the security posture of an organization. In addition to providing robust post-incident forensic capabilities, areas that need attention can be identified and addressed. This creates a feedback loop that makes both defense and post-incident analysis more effective.

Analysis

Knowing the operating parameters of a system can allow for great insight into its operation. Everything from overall system performance, to predictive models for identifying when a fault is imminent, can be discovered through data analysis when given enough inputs of relevance.

The result of the analysis is assurance and auditability. Organizations will have the ability to validate what occurred, and when, provides the ability to easily audit a system. An immutable ledger allows events to be stored in such a way that each corresponding event is cryptographically tied to all the events that occured before it. Changing any event invalidates all

subsequent events in the chain. This, combined with cryptographically signed events, is a very powerful mechanism for tracking system state both in realtime and historically.

How Does Value Stream Management Increase Cyber Resiliency in Software Supply Chains?
Copado believes that good data is fundamental to good cybersecurity. With more accurate and specific data, the better a given tool can be. Value stream mapping tools work by gathering data from each component and process in the SDLC. The collected data can then be sorted for forensic and auditing purposes.

SBOM Integration
These forensic tools could have a significant impact on Software Bill of Materials (SBOM) and other software supply chain requirements that are expected to be announced in the coming months. SBOM will illuminate and track component parts of software. By integrating the output hash of VSM into the SBOM standard as a record of the chain of evidence of software creation, an immutable record of the development process which can later be forensically examined. If the record on file does not match the cryptographically verified record from the software developer/creator, evidence of a problem exists that can be more closely examined for attribution. Copado acknowledges that further development and research is required in this area to create a standard way to sign data to be certain of its provenance but early signs show promise in this area.

VSM Event Standard
Copado is already gathering multiple organizations together to build a standard on how to capture Value Stream Mapping Events. These events will hold consistent information around, time, identity, and reporting system. The more consistent this event standard can be, the stronger interoperability will be between VSM platforms.

Conclusion
Copado would again like to recognize the achievement of value stream mapping as an inclusion to the Secure Software Development Framework (SSDF) and would like to encourage NIST to consider this practice as part of the next iteration on the Cybersecurity Framework.
Value stream management represents the next leap forward in creating a more secure cyber environment. Previously, cybersecurity was taxing on the business and made solely the responsibility of the CISO. Value stream management finds security through transparency. Rather than being onerous if value stream management is adopted as a best practice, it holds the potential to improve not only security, but also the greater efficiencies of the business.