sonatype

The Global Regulatory Landscape for the Software Supply Chain in 2023

CIO and CISO

Compliance Considerations

Recent software supply chain attacks have illuminated the potential for widespread impact on citizens and economies, which have spurred governments around the world to take action. The United States Presidential Executive Orders of February 2021 and May 2021 shined a light on the growing sophistication and intensity of cyber threats and the necessity for software supply chain integrity.

What started as an effort to protect the critical U.S. federal systems from cyberattacks has turned into an expanding resolve by world governments for better rules and management. This means software development organizations who are prepared for this shifting landscape have a competitive edge.

Sonatype's overview of today's global regulatory landscape can share insights into your business' crucial territories. Delays in reacting to software regulations could represent anywhere from missed deadlines to loss of sales, fees, or litigation.

Global

Software Liability

Global consumer protection efforts to date have centered around food, drugs, medical devices, and safety equipment. Software has largely been excluded from this. However, as software is everywhere and a crucial part of the global economy, flaws and problems in software have very real-world consequences.

Most organizations that needed to purchase additional protection had to make a separate arrangement with software companies. For example, a "Service Level Agreement" would require certain basic standards to be met, including security concerns. However, most damages from major outages or software failures are capped and are rarely publicized.

Today, as more and more of our world is software based, people across a spectrum of industries are seeing genuine harm both for citizens and economies coming from software security flaws. The European Union's long-standing GDPR requirements push organizations to "implement appropriate technical and organizational measures." These must "ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services". [1]

This broad declaration is now seeing a more specific declaration to address both software update management and AI/ML.

The goal is "a legal framework to sue the manufacturer for people who suffered material damage, like a physical injury or damage to property, while using a certain product".[2]

In the U.S., the Biden-Harris Administration's National Cybersecurity Strategy in March 2023 includes a call for cybersecurity liability. Proposed rules seek to hold software providers and data responsible for breaches. To help in this effort, the strategy also discusses a re-alignment of incentives to favor long-term investments in cybersecurity. The strategy is effectively a call to

[1] Source: Article 32 GDPR "Security of processing"

[2] Source: Regulating the future: A look at the EU's plan to reboot product liability rules for AI

action for federal agencies and private sector companies to build and mature a digital ecosystem. One that is more resilient against cyber attacks and better serves society.

- ▶ Easily Stop Malware, Before Your Company Becomes Liable
- ▶ Read the full National Security Strategy recap.
- ▶ More on Software Liability

Commercial Sector

In **June 2022**, the International Medical Device Regulators Forum (IMDRF)'s Cybersecurity Working group issued "Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity." This work looks to mitigate safety risk through the life cycle of a medical device, specifically looking at a software bill of materials (SBOM) through the lens of both pre-market activities (see later in this article for what the U.S. Food and Drug Administration (FDA) has already put in place), as well as postmarket activities, saying:

> "During the life cycle of the medical device, both the author...and the recipient...of the SBOM rely on accurate and up-to-date information about the third-party software components to identify and mitigate potential patient safety risks associated with possible third-party software vulnerabilities on the device or systems in which the devices operate."

There are potential parallels with the EU Cyber Resilience Act (CRA), given that the IMDRF guidelines are looking at the device's lifetime, which speaks to the need for ongoing vulnerability management.

Initiatives around the world

United States

Turning the Presidential Executive Orders of 2021 into action has been the focus throughout much of 2022, with deadlines peppered throughout 2023.

FEDERAL AGENCIES – 2023 DEADLINES

In September 2022, the Office of Management and Budget (OMB) issued the Memorandum: "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," also called M-22-18, which set 2023 deadlines for self-attestations of software used by federal agencies. (Attestations for critical software are due in July 2023, and all other software by September 2023.) Further, the memorandum says:

"SBOMs may be required by the agency in solicitation requirements, based on the criticality of the software as defined in M21-30, or as determined by the agency."

OMB directs federal agencies to follow SBOM guidance from the National Telecommunications and Information Administration (NTIA) in the report "The Minimum Elements for a Software Bill of Materials (SBOM)." The National Institute of Standards and Technology (NIST)'s role in software supply chain security was codified in the CHIPS Act of 2022.

FEDERAL AGENCIES – 2024 DEADLINES

"Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," also called M-22-09, set an end-of-2024 fiscal year deadline for agencies to meet specific cybersecurity standards and objectives in accordance with the Presidential Executive Orders of 2021. The OMB specifically advised agencies to align with the Cybersecurity and Infrastructure Security Agency (CISA)'s Five-Point Zero Trust Model.

Additionally, agencies already complete a Security Assessment Report (SAR) as part of the authorization process for information systems. The OMB wants to lean further into this application security testing by evolving the SARs to include "not just information gathered by automated tools for vulnerability scanning and code analysis of custom-developed software, but also analysis prepared by more time-intensive, specialized, and application-specific methods." To help accomplish this, OMB advised agencies to follow the NIST July 2021 "Guidelines on Minimum Standards for Developer Verification of Software."

As a follow up to the July minimum standards publication, in February 2022, NIST followed up with "Software Supply Chain Security Guidance Under Executive Order 14028.". The document provided guidance and best practices for securing the software supply chain. Specifically, it introduced the concepts of "attestation" (a statement that requirements have been met) and "artifact" (a piece of evidence).

> "When a federal agency (purchaser) acquires software or a product containing software, the agency should receive attestation from the software producer that the software's development complies with government-specified secure software development practices. The federal agency might also request artifacts from the software producer that support its attestation of conformity with the secure software development practices."

While this covers the point of purchase, it then goes a step further into the source of the problem. Given the "dynamic nature of software development," NIST highlights the need for ongoing attestation performed "…as part of the processes and procedures throughout the software lifecycle."

In May 2022, NIST provided additional, comprehensive guidance in "Software Security in Supply Chains" related to the "acquisition, use, and maintenance of third-party software". The guidance also offered recommended concepts and capabilities spanning SBOM, vendor risk assessments, open source software controls, and practices for vulnerability management.

Some of the sustaining capabilities highlighted include:

- Binary **software composition analysis** (SCA) to identify vulnerable components, specifically those that include open source
- Set up and maintain **one or more repositories** and/or libraries of open source software for developer use.

DEVELOPMENT TEAM GUIDANCE

In September 2022, The National Security Agency, CISA, and the Office of the Director of National Intelligence (ODNI) released Securing the Software Supply Chain: Recommended Practices Guide for Developers. It specifically highlighted the changing nature of threats and the outsized and pervasive impact of malicious code:

> "A traditional software supply chain cycle is from point of origin to point of consumption and generally enables a customer to return a malfunctioning product and confine any impact. In contrast, **if a software package is injected with malicious code which proliferates to multiple consumers; the scale may be more difficult to confine and may cause an exponentially greater impact.** Common methods of compromise used against software supply chains include exploitation of software design flaws, incorporation of vulnerable third-party components into a software product, infiltration of the supplier's network with malicious code prior to the final software product being delivered, and injection of malicious software that is then deployed by the customer."

There are a number of practical mitigation measures to mitigate the risk of intentional or unintentional malicious code injection.[3]

- A well-balanced authenticated source control check-in process, including **protection of the source code repository**. Recommended protections include a lot of all developers and the components they download.
- Automatic **static and dynamic vulnerability scanning on all components** of the system. They also recommend that "separate and higher quality scanning tools should also be used within the product build environment."
- Conducting **nightly builds with security regression tests**.
- The **mapping of development efforts to specific system requirements**. This helps avoid "feature creep" that could inject vulnerabilities.
- Employing both informal and formal **code reviews**.
- Continuous **training for developers in secure development practices**.
- **Hardening the development environment**, using the similar approaches one would use to protect production systems.

[3] Source: Securing the Software Supply Chain: Recommended Practices Guide for Developers

LEGISLATIVE MOVEMENT

In March 2023, Representative Gary Peters introduced the Securing Open Source Act of 2023 (S. 917). While its primary function is to establish the duties of the Director of CISA as they relate to open source security, the bill also recognizes the intrinsic value of open source, specifically saying:

> "… a secure, healthy, vibrant, and resilient open source software ecosystem is crucial for ensuring the national security and economic vitality of the United States."

Within one year of the enactment of the legislation, the Director of CISA is called upon to:

> "…publicly publish a framework, incorporating government, industry, and open source software community frameworks and best practices, including those published by the National Institute of Standards and Technology, for assessing the risk of open source software components, including direct and indirect open source software dependencies."

Sonatype has established a resource that answers many common questions around software dependencies, both direct and indirect.

Also in March 2023, the AI for National Security Act (H.R. 1718) was introduced, specifically calling out "enhancing the security of the software supply chain" as it relates to America's Department of Defense.

LAWS PASSED

In June 2022, the Supply Chain Security Training Act of 2021 became law. This directs the Federal Acquisition Institute to develop a training program that "mitigate[s] supply chain security risks that arise throughout the acquisition lifecycle, including for acquiring information and communications technology. The Supreme Court Security Funding Act of 2022, which became law in August 2022, specifically calls out software supply chain security practices. Other Bills, such as the DHS Software Supply Chain Risk Management Act of 2021, continue to move through the legislative process and focus on the supply chain as the key element in strengthening cybersecurity.

The Supply Chain Security Training Act directs the Federal Acquisition Institute to develop a training program that: "mitigate[s] supply chain security risks that arise throughout the acquisition lifecycle, including for the acquisition of information and communications technology."

INDUSTRY-SPECIFIC INITIATIVES

In March 2022, the Securities and Exchange Commission (SEC) issued a proposed rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. This could require public companies to make public disclosures to investors about cybersecurity incidents within days of the discovery. The SEC specifically called out that "cybersecurity incidents involving third-party service provider vulnerabilities are becoming more frequent" as one of the key drivers behind this rule proposal. In March 2023, they followed up with a more definitive ask:

> “The proposal would require all Market Entities to implement policies and procedures that are reasonably designed to address their cybersecurity risks and, at least annually, review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review.”

Further, they would need to file annual disclosures of cybersecurity risks and incidents incurred during the previous year.

In April 2022, the Food and Drug Administration (FDA) sought comment on medical device cybersecurity in “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.” Specifically, it recommended replacing “Cybersecurity Bill of Materials” with SBOMs on pre-market submissions. The IMDRF took note.

More information is available in the Global Commercial Sector section of this document.

In March 2023, the FDA followed up with a new rule. Beginning October 1, 2023, new medical device applications or submissions must be accompanied by SBOMs “… including commercial, open-source, and off-the-shelf software components.” Even more critical is the requirement for ongoing monitoring of “postmarket cybersecurity vulnerabilities and exploits,” including the “processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems to address.”

For those companies, Sonatype produced a presentation on SBOMs: The Future in Healthcare.

Idaho National Laboratory (INL), which is associated with the U.S. Department of Energy, continues the work it initiated in 2021 on Energy sector SBOMs. This includes its S4x23 SBOM Challenge, the results of which INL shares on its website.

Canada

In June 2022, the Canadian government completed a first reading of Bill C-26, titled “An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.” While the bill specifically pertains to telecommunication service providers, it would require them to “manage any organizational cyber security risks, including risks associated with the designated operator’s supply chain and its use of third-party products and services.”

Despite this initial legislative focus on a specific vertical, data shows that software supply chain integrity is a concern across the broader Canadian business community. In its “2023 Canadian Digital Trust Insights” survey, PricewaterhouseCoopers reported that 87% of respondents say they’re experiencing greater demand for cyber incident disclosures. Still, only 43% say they can provide the required documentation on incident reporting.

United Kingdom

In December 2022, the UK Government updated the National Cyber Security Strategy 2022 it initially unveiled in February 2022. This policy specifically cites supply chain vulnerabilities as an area of concern. The strategy specifically tasks the Department for Digital, Culture, Media, and Sport (DCMS) with implementing Network and Information Systems (NIS) regulations in coordination with the National Cyber Security Centre. Further revision is likely as the NIS Regulations were last updated in 2020. The 2022 through 2030 strategic document is available.

In July 2022, the UK government issued a Proposal for Legislation to "Improve the UK's Cyber Resilience." It then followed it up with a February 2023 call for views on software resilience and security for businesses and organizations.

Australia

In March 2023, the Australian Cyber Security Centre (ACSC) issued Guidelines for Software Development. Specifically, the guidelines call for Application Security Testing (AST) with specific focus on helping developers identify vulnerabilities. The guidelines also specifically call out the need for a Software Bill of Materials (SBOM). ACSC points to several United States' NTIA assets for further guidance, including documents on cyber supply chain transparency and The Minimum Elements For a Software Bill of Materials (SBOM) publication.

More on Sonatype's suggestions around AST.

European Union

In September 2022, the European Union released the Cyber Resilience Act (CRA), intended to "bolsters cybersecurity rules to ensure more secure hardware and software products." It is similar to other legislation in its call for SBOMs, but where it takes it a critical step further (similar to the new U.S. FDA rule) is the requirement for corrective measures – comparable to a manufacturer's recall, but for security.

After issuing its landmark 2021 report titled "Understanding the increase in Supply Chain Security Attacks," which reviewed 24 different software supply chain attacks, European Agency for Cyber Security (ENISA) shared its "Cybersecurity Threat Landscape Methodology" report in July 2022, making an example of supply chain threats. They followed this up in February 2023 with detailed guidelines on Developing National Vulnerability Programmes. The guidelines advocate for a security-by-design approach and highlighted automated prioritization and treatment of vulnerabilities as an ongoing challenge.

Sonatype has written about vulnerability priority and security by design.

Further, the European Union joined the United States government to launch the U.S.-European Union Trade and Technology Council. While their May 2022 statement would suggest their initial focus is on supply chain resiliency around critical components, such as semiconductors, the broader plan points to cross-continent collaboration around the broader software supply chain with an eye toward protecting national security. In December 2022, the Council broadened the focus to Artificial Intelligence (AI).

In May 2022, European Parliament and European Union Member States reached an agreement on New Rules on Cybersecurity of Network and Information Systems, which advocates for a high common level of cybersecurity across the European Union. This, known as the NIS 2 Directive, was officially adopted in January 2023.

Among other things, NIS 2 talks about the necessity of open source through the lens of value and security:

> "Member States should therefore be able to promote the use of open-source software and open standards by pursuing policies relating to the use of open data and open-source as part of security through transparency. Policies promoting the introduction and sustainable use of open-source cybersecurity tools are of particular importance for small and medium-sized enterprises

> facing significant costs for implementation, which could be minimised by reducing the need for specific applications or tools."

Japan

Japan passed "Act on Promotion of Economic Security by Integrated Implementation of Economic Measures," landmark national security legislation, in May 2022. The act has four main pillars, with the first two focused on supply chain stability and security for critical infrastructure, the latter said to be modeled on the U.S. and German approaches. The law is expected to take effect on or before February 2023.

In August 2022, the Open Source Security Summit came to Japan. Hosted by the Linux Foundation and Open Source Software Security Foundation (OpenSSF) and under the auspices of the Ministry of Economy, Trade, and Industry, the event served as a follow-up to May 2022's Open Source Software Security Summit II, Following the Executive Orders of 2021, these industry groups, in association with the White House's National Security Council and prominent technology companies, have collaborated on a 10-Point Open Source and Software Supply Chain Security Mobilization Plan, which advocates for "SBOM Everywhere" along with "better supply chain security tools and best practices."

> "While reliance on software technology, including OSS [Open Source Software], is increasing, software management methods, vulnerability handling and license support are becoming increasingly important, such as the announcement of the Log4j vulnerability. As I will introduce today, the Ministry of Economy, Trade and Industry is also making various efforts to ensure the security of software including OSS, by developing a collection of practices for OSS management methods and conducting a demonstration of the use of SBOM. Through this meeting, we hope to deepen our knowledge of software security including OSS, and to promote more active efforts in Japan to resolve issues such as management methods and vulnerability countermeasures."
>
> **–KEYNOTE SPEAKER MASAHIRO UEMURA'S REMARKS AT THE OPEN SOURCE SOFTWARE SECURITY SUMMIT, HIGHLIGHTING JAPAN'S RECENT EFFORTS, AS WELL AS UNDERSCORING THE URGENCY TO ADDRESS OPEN SOURCE VULNERABILITIES**

Indo-Pacific

In May 2022, the Prime Ministers of Australia, India, Japan, and the President of the United States a group known as the Quad) announced a collective approach to addressing cybersecurity issues:

> "To deliver on the Quad Leaders' vision for a free and open Indo-Pacific, we commit to improving the defense of our nation's critical infrastructure by sharing threat information, identifying and evaluating potential risks in supply chains for digitally enabled products and services, and aligning baseline software security standards for government procurement, leveraging our collective purchasing power to improve the broader software development ecosystem so that all users can benefit.

The group has also collaborated on a "Common Statement of Principles on Critical Technology Supply Chains," which aligns around four key principles: Security, Transparency, Autonomy, and Integrity. The Quad's activities will continue to be coordinated under the banner of the Quad Cybersecurity Partnership. Their next in-person meeting is in 2023.

Anticipating Future Changes

Since the Executive Order, the inertia behind regulation has only increased. Some changes on the horizon seem almost inevitable. Some specific changes we expect:

Growing specificity in terms of requirements that would impact software manufacturers and businesses, starting with SBOMs and likely later expanding into ongoing vulnerability management. Particularly those that are publicly traded and/or in regulated industries.

In the healthcare space, escalating intensity around ongoing vulnerability disclosures through the lens of both financial risk and patient care.

For federal agencies, growing specificity around software supply chain requirements.

Regulatory debt

Today, software security and reliability are increasingly top-of-mind for leaders worldwide. As governments try to react to the dangers and protect commerce, new requirements are a crucial consideration for development teams.

When new rules and regulations go live, will your organization be caught off guard, take a band-aid approach, or can you quickly adopt the latest best practices? Software development that ignores these new challenges risks falling behind.

Sonatype will continue to explore regulatory requirements affecting the software supply chain to help our customers and the industry meet a better software future.

Headquarters
8161 Maple Lawn Blvd, Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place, Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com