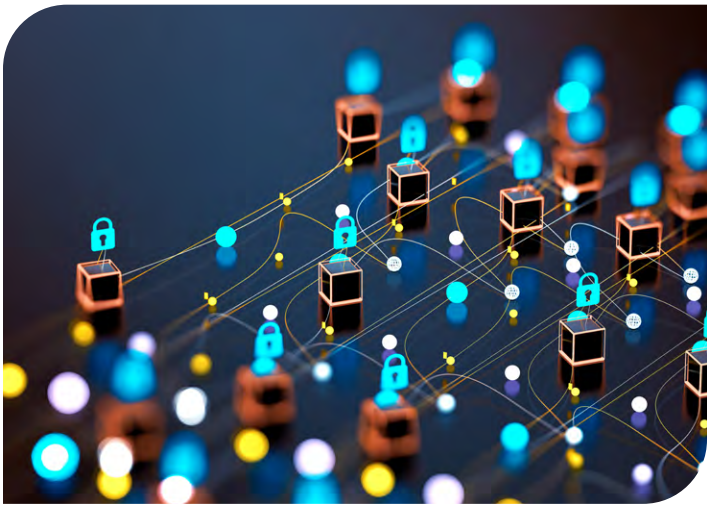
Navigate the Executive Order 14028 Era of Software Security: Guidance from SAFECode

01010
0100000
010001
01000
0100001

SAFECode

Introduction



May 12, 2021 was a pivotal moment in cybersecurity history. The White House published Executive Order 14028 (EO 14028), a landmark document with an aggressive stance designed to advance the cybersecurity conversation[1]. While the document focuses on US federal government agencies and the companies that supply them, it's a useful reference for those around the world who want to follow best practices in cybersecurity.

EO 14028 has significant real-world ramifications for vendors selling software to the federal government, adding stringent security guidelines when selling software and cloud services to federal agencies. Adherence to those guidelines is likely to trickle down to the rest of the US economy. It demonstrates cybersecurity leadership by example.

As the key agency pursuing excellence in information science, the government asked the National Institute of Standards and Technology (NIST) to handle many of the tasks supporting EO goals including software supply chain security. NIST responded to this direction by updating its Secure Software Development Framework (SSDF) to version 1.1[2].

The SSDF is a comprehensive document outlining best practices in software development security, and it draws on a wide range of industry expertise. The project to create it launched in a public session at the RSA Conference in 2018. SAFECode's executive director Steve Lipner co-moderated that session along with Donna Dodson, who was then chief cybersecurity advisor at NIST's Information Technology Laboratory.

It is perhaps no wonder that the SSDF draws heavily on SAFECode's own Fundamental Practices for Software Development (FPSSD), the third version of which was released publicly in 2018. This document contains many elements that informed both the EO and the SSDF. We recommend it as a comprehensive guide for software vendors wishing to meet the requirements of the EO, and indeed for any company that wants a sound perspective on secure software development. This document is a useful complement to NIST's own work.

The origins and history of SAFECode's FPSSD

Originally called the Software Assurance Forum for Excellence in Code, SAFECode was formed in 2007 by a group of technology companies to focus on secure software development practices. The founding members recognized the need for a coordinated effort to improve the security of the software that is used by millions of people around the world.

We bring together industry experts and researchers to share expertise about secure software development. We complement our work on secure coding by raising awareness about the importance of software security and publishing free training courses to guide developers. By educating the broader public and policymakers about the risks and consequences of insecure software, we aim to promote greater adoption of secure coding best practices and help organizations create a safer, more secure digital world.

1 House, The White. "Executive Order on Improving the Nation's Cybersecurity." The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

2 Computer Security Division, Information Technology Laboratory. "SSDF v1.1: Draft SP 800-218 Available for Comment | CSRC." CSRC | NIST, September 29, 2021. https://csrc.nist.gov/News/2021/ssdf-draft-sp-800-218-available-for-comment.

Our Fundamental Practices for Secure Software Development (FPSSD) is a critical part of this effort. Originally published in 2008, this document distils the best practices involved in creating a secure development lifecycle (SDL) as implemented every day by our members.

We designed this collection of "practiced practices" with simplicity and actionability in mind. The goal was to ensure that developers and security professionals could produce fast results that hardened their software against attack.

Since then, we have issued two major updates to the document. The second edition, published in 2011, offered a deeper focus on secure software design, development, and testing with expanded guidance. We added a discussion of sandboxing into the design stage and made it easier to map coding practices against software security weaknesses by adding Common Weakness Enumeration (CWE) references to our listed practices. Another addition - verification guidance - helped organizations to close the circle by checking that developers had implemented our recommendations properly.

In 2018 we updated the document again. The third edition updates the fundamental SDL practices to address a dynamic industry with rapidly evolving risks. It adds discussions including considerations for deployment of secure development practices in an organization, requirements identification, security issue management, and vulnerability response and disclosure. It also addresses the management of third-party software components.

How the FPSSD aligns with the requirements of EO 14028

EO 14028 is a response to a rising cybersecurity threat that has plagued the federal government and many contractors. The US government has seen thousands of security incidents that were becoming an increasing threat to its own operation and to the critical infrastructures of the country.

The US Government Accountability Office designated information security as a government-wide high-risk area in 1997, later expanding it to include critical cyber infrastructure and personally identifiable information. However, the security incidents keep coming. In 2021, the Department of Homeland Security received over 32,000 security incident reports from federal agencies. These ranged from web-based attacks to phishing[3].

Some of these attacks were catastrophic. Between 2013 and 2015, the Office of Management and Budget (OMB) suffered a massive attack by a foreign actor, resulting in the theft of millions of citizens' detailed personal information[4].

In 2020, US government contractor SolarWinds suffered from an attack on its software build systems that allowed foreign actors to compromise software used by dozens of federal agencies[5].

The rising problem prompted the White House to release an EO with teeth. It went beyond mere guidance to demand compliance from federal agencies and their suppliers in several key areas. It also mandated the removal of government contracts that failed to comply with the new rules.

3 Office, U. S. Government Accountability. "Cybersecurity." Accessed December 8, 2022. https://www.gao.gov/cybersecurity.

4 Fruhlinger, Josh. "The OPM Hack Explained: Bad Security Practices Meet China's Captain America." CSO Online, February 12, 2020. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

5 Jaikaran, Chris. "SolarWinds Attack—No Easy Fix," n.d., 3.

The EO mandates protective measures in several areas, including information sharing and modernizing operational cybersecurity practices for federal agencies. However, the part that aligns most clearly with SAFECode's own work is section four: Enhancing Software Supply Chain Security. This establishes new guidelines for evaluating software and developer security across several important areas.

Software development environments

The EO is astute in its call to secure both the software development process and the technical tools that developers use to create software. Software security begins with the tools used to create it, and poor security in the choice and configuration of those tools can create gaping security holes for attackers to exploit. For example, the SolarWinds attackers poisoned the software after gaining access to the company's deployment pipeline and inserting malicious code, which shows the dangers of inadequately securing these environments.

The FPSSD addresses software development environment security including the use of appropriate compiler and toolchain versions. It emphasizes the use of secure compiler configuration options. It links to detailed resources for toolchain configuration and recommends tools to harden Linux, Apple, and Windows application code.

Automating source code security checks

The EO also calls for automated discovery and mitigation of software security flaws as part of the developer's tooling. This is a focal point for the FPSSD, which dedicates an entire section to testing and validation. Our discussion of code analysis tools covers both static and dynamic analysis, along with fuzzing and both automated and manual security testing, including penetration testing.

Multi-factor authentication

The EO prompts agencies to establish multi-factor authentication and access controls to protect enterprise software and the systems that create it. The FPSSD has a section dedicated to standardizing identity and access management that includes advice about how to authenticate not just users but also services. Service authentication is an important factor in the kinds of machine-to-machine transactions that we find in cloud-based environments that use APIs and microservices. We also advise developers and administrators on how to store and rotate authentication credentials.

The FPSSD distinguishes between authentication and authorization, the latter being an important factor in another of the EO's stipulations: zero-trust architecture. We advise organizations on how to authorize all users against all services using a least-privilege policy.

Documenting dependencies

Software dependencies have become a huge part of the software security discussion. The discovery of the Log4Shell vulnerability in November 2021 was a case in point, affecting large portions of the Internet because of Log4J's ubiquity in so many products[6].

The EO explicitly calls for agencies to document dependencies as part of the software security effort, and the FPSSD addresses the management of third-party component vulnerabilities. Another SAFECode guide, Managing Security Risks Inherent in the Use of Third-Party Components, goes deeper still[7].

The EO also calls for agencies to use a software bill of materials (SBOM) to help track the underlying components of the software they use. SAFECode has always stressed that developers should track and manage their components and is engaged with organizations that are working on SBOM frameworks applications.

Proving compliance

The EO requires agencies to demonstrate that they have achieved the goals that it sets out. Compliance is a challenge for many organizations beyond government agencies and documenting secure development actions can be time-consuming and difficult. The FPSSD advises on reducing this 'compliance tax' by generating much of this information as an artifact from correctly configured tool sets during the development process.

Protecting critical software in production

The SDL doesn't end at deployment. The EO describes the need to identify critical software and then apply key principles to protect it in production, such as network segmentation, network vulnerability scanning, and proper configuration.

SAFECode advises developers to secure their software through effective configuration, including correctly setting file protections and closing unused network ports by default. These tasks have direct payoffs in terms of operational security.

Encrypting data

The EO acknowledges the importance of data encryption to both the software development and production environments, calling upon NIST to issue guidance on this point. The FPSSD has recommendations both for encryption in-transit and at-rest, along with key management. It also explores the fast-moving evolution of cryptography, advising organizations to evolve their cryptographic agility so that they can cope with future changes to the computing landscape. This recommendation is especially critical given the emerging threat to cryptography of quantum computers – the subject of a 2022 National Security Memorandum and Executive Order[8].

6 "CVE Record | CVE." Accessed December 9, 2022. https://www.cve.org/CVERecord?id=CVE-2021-44228.

7 Licata, Scott. "Managing Security Risks Inherent in the Use of Third-Party Components." SAFECode, May 8, 2019. https://safecode.org/resource-secure-development-practices/managing-security-risks-inherent-in-the-use-of-third-party-components/.

8 "FACT SHEET: President Biden Announces Two Presidential Directives Advancing Quantum Technologies", May 4 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/

Managing vulnerability disclosure programs

Even with the best secure development process and automated tooling, software security vulnerabilities still crop up in production. The EO calls for disclosure mechanisms to ensure that agencies collect these bugs from researchers and act upon them.

The FPSSD explores applicable standards for managing disclosure programs. It focuses on ISO/IEC 29147 and 30111 as it explores the creation of internal and external policies along with the roles and responsibilities to support them.

SAFECode outlines best practices in vulnerability reporting and disclosure including:

- Providing clear reporting guidelines and contacts for vulnerability reporting.
- Establishing a standard for acknowledging reports and keeping reporters briefed.
- Vulnerability triage and mitigation.
- Vendor vulnerability disclosure, including multi-party coordination.

Minimum vendor testing standards

The EO calls for guidelines that agencies can use to mandate minimum software security testing standards for vendors. Since edition two, the FPSSD has supported software vendors by providing best practices for verifying the security of their software. These now include evaluating security controls and assessing the security test cases for their software, along with the test results. The document describes verification as part of a four-stage process for managing software development risk.

Incident investigation

When software security incidents inevitably occur, it is important for all organizations to close the circle, exploring the reasons for any incidents and then evaluating and mitigating their impact. Incident investigations should allow organizations to reduce the chance of similar incidents occurring in the future.

The EO acknowledges the importance of incident investigation and takes a significant step to address it, creating the Cyber Security Review Board to take responsibility for it. Part of this mandate includes ensuring that software vendors collaborate fully with incident investigations.

The FPSSD pays special attention to incident investigation and response, offering advice and further resources on learning and applying lessons from incidents in its section on secure development lifecycle feedback. This guidance not only helps to avoid specific recurring software security issues, but also contributes to the overall health of the SDL by creating continuous improvement opportunities using feedback loops based on software development process data.

Going beyond the EO requirements

The EO provides a valuable guide to software security for government agencies, their suppliers, and by implication other organizations. NIST's corresponding update to the SSDF does an excellent job of addressing these issues.

However, organizations must still work out how to interpret and execute the list of requirements in both of these documents to create an internal secure development process that they can implement and manage. The SSDF provides a resource to organizations that are trying to follow the guidance in the SSDF and EO by exploring the broader cultural and organizational requirements of an effective secure software development program.

These discussions encompass the planning of an SDL from end to end, including some of the less tangible but equally important challenges. For example, organizations must integrate organizational culture into the SDL (see SAFECode's Security Champions Guide for reference) and the SDL into organizational culture. Any successful initiative needs people to implement it. It should acknowledge their needs and also explore what has and has not aligned effectively with corporate culture in the past.

Acknowledging and aligning with corporate culture also means managing and communicating with stakeholders effectively. Those stakeholders must have the necessary skills in place to support and advance a secure development initiative.

Conclusion

Organizations should prepare now for a far greater emphasis on software security as a result of the EO. NIST and other organizations such as OWASP are good places to start for complementary guidance on how to comply with its requirements.

We also suggest the FPSSD and our other complementary papers as go-to documents for a deep dive into secure software development and software supply chain security. They offer best practices that align well with those from other organizations, but which come from experts that apply them daily in the field.


01010
0100000
010001
01000
0100001
SAFECode
Driving security and integrity.