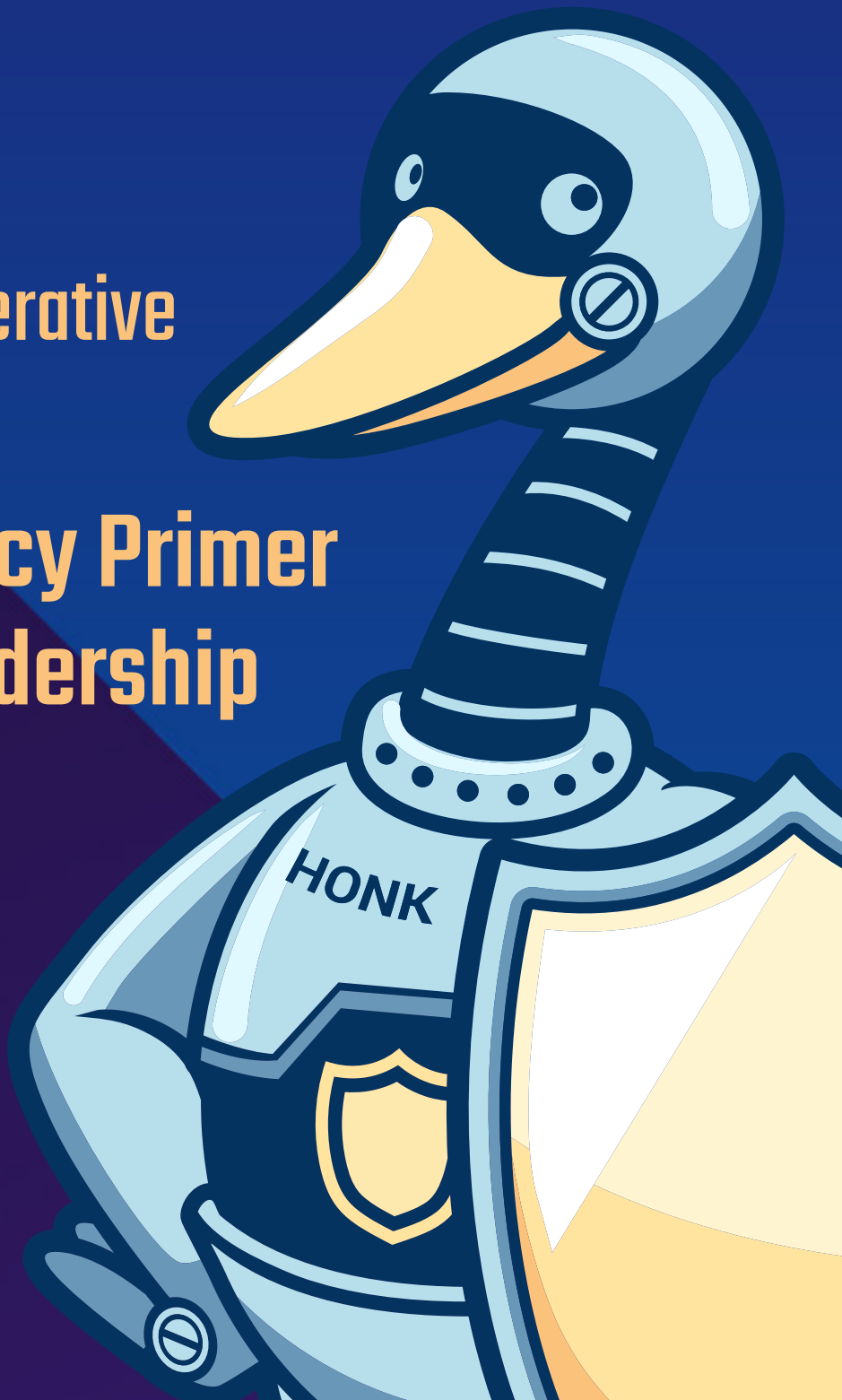
OpenSSF

OPEN SOURCE SECURITY FOUNDATION

The Economic and Security Imperative of Open Source Software: A Policy Primer for Global Leadership



openssf.org

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Contents

The Economic and Security Imperative of Open Source Software: A Policy Primer for Global Leadership

Open source software (OSS) is a critical digital foundation that underpins and advances economic and national security. OSS is embedded across the modern economy, including proprietary products, with audits finding OSS present in 96% of commercial codebases.[1] OSS is "software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and redistribution by the users of such software."[2] This document provides an overview of OSS' economic and security benefits and outlines recommendations for maximizing OSS value through deepened public-private collaboration.

The Open Source Security Foundation (OpenSSF) is a cross-industry initiative under the Linux Foundation dedicated to improving the security of open source software. It brings together a broad set of stakeholders, including leading technology companies, security researchers, and public sector participants, to collaborate on practical security improvements, tooling, standards, and best practices. OpenSSF's work focuses on strengthening the security of widely used open source components that underpin both commercial and government systems, reflecting a shared interest across the software ecosystem. Its projects and working groups address areas such as vulnerability disclosure, supply chain security, secure development practices, and incident response, making it a credible, practitioner-driven forum for advancing software security at scale.

1. Synopsys, *2024 Open Source Security and Risk Analysis (OSSRA) Report,* https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

2. US Department of Defense (2022), "Software Development and Open Source Software", https://dodcio.defense.gov/portals/0/documents/library/softwaredev-opensource.pdf

Key Takeaways for Policymakers

- In both open and proprietary systems, OSS is embedded as a ubiquitous software component.
- Targeted public and private investment in widely used OSS components delivers systemic risk reduction.
- Policies that fragment OSS ecosystems or shift liability to OSS developers will weaken security.
- AI development depends heavily on OSS infrastructure and, increasingly, AI is being applied to improve OSS security; policies should support both dynamics.

OSS' Economic Value and Innovation Impact

Open source software is not a niche technology. It is embedded in virtually every layer of the modern digital economy, driving innovation, reducing costs, and enabling global competitiveness.

- OSS is embedded across the modern economy, including proprietary products, with audits finding it present in 96% of commercial codebases, making it foundational infrastructure for the entire digital economy.[3]
- OSS enables broad reuse of common components, reducing duplicative development and allowing firms to compete and innovate at higher layers of the technology stack. The demand-side value of widely-used OSS totals $8.8 trillion globally.[4]
- OSS is foundational to AI development: the dominant ML frameworks (PyTorch, TensorFlow), model-serving infrastructure, and training pipelines. Increasingly open weight models are key components of business applications.
- Firms that adopt and contribute to OSS can achieve measurable productivity gains, particularly where they build complementary capabilities and participate in OSS ecosystems.[5]
- OSS activity contributes to innovation and competitiveness by enabling knowledge spillovers, lowering barriers to entry, and supporting new firm formation and technological independence.[6]
- The global OSS ecosystem relies on companies, foundations and developers from multiple regions that are central to the development and stewardship of widely used projects.

3. Synopsys, *2024 Open Source Security and Risk Analysis (OSSRA) Report,* https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

4. Hoffman, J., Nagle, F., & Zhou, Y. (2024). *The Value of Open Source Software.* Harvard Business School Strategy Unit Working Paper No. 24-038. https://www.hbs.edu/faculty/Pages/download.aspx?name=24-038.pdf

5. Frank Nagle, "Open Source Software and Firm Productivity," *Management Science* 65, no. 3 (2019): 1191–1215. https://ideas.repec.org/a/inm/ormnsc/v65y2019i3p1191-1215.html

6. Knut Blind et al., The Impact of Open Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy (European Commission, 2021).

OSS Security is a Collaborative Enterprise

Securing open source software is not the responsibility of any single actor. It is achieved through shared practices and investments across maintainers, commercial users, and public-sector participants.

- OSS security is produced through collaboration among maintainers, commercial and non-commercial users and contributors, and public-sector actors, rather than any single development model; many widely used components are maintained and secured jointly by industry and community contributors.
- Common security practices such as code review, automated testing, vulnerability disclosure, and coordinated patching are implemented across OSS and proprietary development, forming a shared baseline for modern software security.
- Because widely used OSS components are shared dependencies, investments in improving their security (e.g., audits, memory safety, fuzzing) reduce risk across many downstream systems simultaneously.
- OSS enables visibility into dependencies and build processes, supporting supply chain security practices such as SBOMs and provenance attestation.

Deployers and Integrators Should be Responsible for Security Outcomes

Responsibility for operational security outcomes rests primarily with deployers and integrators, who select, configure, and maintain software in specific environments, regardless of whether components are open or proprietary.

- Final assemblers are best positioned to manage risk. Organizations that assemble open source components into products and services are typically more mature, better resourced, and better equipped to evaluate whether a given component is fit for purpose in their specific context. Original open source creators are often unaware of how their code will ultimately be used, making it impractical to hold them accountable for downstream deployment decisions.
- Liability should not roll downhill to volunteer maintainers. Many critical open source projects are maintained by individuals or small teams on an entirely voluntary basis. Imposing security liability or compliance costs on these contributors, rather than on the well-resourced organizations that profit from integrating their work, would discourage the very contributions that make the software ecosystem more innovative and secure.
- Deployers control the update and patching lifecycle. The most persistent security risks stem not from flaws in code, but from the failure to apply known fixes. As the Log4j vulnerability demonstrated, even after patches are available, vulnerable versions can continue to be downloaded hundreds of thousands of times daily. Deployers and integrators, not upstream maintainers, control whether and when security updates reach production environments.

Three Roles for Government in Securing Open Source Software

Government as Security-Focused Consumer

Governments are among the largest consumers of software built on open source components. Treating those components as critical dependencies and investing in their security accordingly, strengthens the resilience of public-sector systems and the broader ecosystem.

- Treat widely used OSS components as critical dependencies in software supply chains, prioritizing their security, maintenance, and long-term sustainability.
- Adopt OSS using risk-based criteria (e.g., project maturity, maintenance, and security practices), not licensing model alone.
- Encourage and implement secure-by-design practices in procurement and deployment, such as SBOMs, vulnerability disclosure, and timely patching.
- Fund targeted security improvements (audits, fuzzing, memory safety, build integrity) in widely used OSS components.
- Establish or strengthen Open Source Program Offices (OSPOs) to manage OSS use, contribution, and risk systematically.

Government as a Participant in a Shared Security Ecosystem

Beyond consuming open source software, governments can actively strengthen the ecosystem by contributing fixes upstream, funding sustained maintenance, and coordinating with industry on shared security standards and practices.

- Contribute security fixes and improvements upstream, ensuring that public investment benefits all users and avoids fragmentation.
- Support sustained funding mechanisms for OSS security and maintenance, particularly for widely used and under-resourced components.
- Enable public–private coordination on vulnerability disclosure, incident response, and security best practices.
- Invest in and adopt shared security tooling and standards (e.g., SLSA, Scorecard) used across both open and proprietary development.
- Promote international alignment on OSS security practices to maintain a globally interoperable and reviewable ecosystem.

Government as Risk-based Regulator

Regulatory approaches to software security should reflect how open source is actually developed and maintained, placing obligations on the parties best positioned to act, while avoiding requirements that would burden volunteer contributors or fragment the global ecosystem.

- Place responsibility for security outcomes on deployers and integrators, who control how software is selected, configured, and maintained in operational environments.
- Avoid imposing direct obligations on upstream OSS developers that are incompatible with decentralized, global development models.
- Avoid contractual pass-through or liability structures that cannot be met by volunteer or non-commercial maintainers.[7]
- Avoid policies that would fragment the global OSS ecosystem, reducing shared review and weakening security.

AI and Open Source Software: An Emerging Policy Intersection

Artificial intelligence and open source software are deeply intertwined. AI systems depend on OSS infrastructure, while AI tools are increasingly being used to improve the security of open source code. Policy should reinforce both dynamics.

- AI systems are overwhelmingly built on OSS components, from training frameworks to inference infrastructure to the growing ecosystem of open-weight models. The security and sustainability of this OSS base layer directly affects the safety and reliability of AI systems built on top of it.
- AI tools are increasingly used to improve software security, including automated vulnerability discovery, code review, and remediation. This creates opportunities for significant security gains in widely used OSS components.
- AI-generated code and autonomous AI agents are also increasing contribution volume to OSS projects, creating new challenges for maintainer capacity and project governance. Policy should support tooling and practices that help maintainers manage these dynamics without closing off beneficial contributions.
- Policymakers should treat open source AI and AI-for-security as complementary to existing OSS policy objectives, not as a separate domain requiring fundamentally different approaches.

7. Open Source Initiative, "AI Policy & Open Source Software" https://opensource.org/blog/new-resource-on-ai-open-source-for-u-s-policymakers

OpenSSF as a Partner for Policy Leadership

OpenSSF is ready to serve as a practical partner for policymakers seeking to strengthen open source security. The foundation already operates at the intersection of the issues outlined in this primer: its Alpha-Omega project, backed by a $12.5 million coalition investment from leading technology and AI companies, has funded over 60 security audits of critical open source components and remediated dozens of vulnerabilities in projects that underpin both commercial and government systems. OpenSSF tools and standards provide the kind of automated, verifiable security infrastructure that government procurement and regulatory frameworks can build on today. At the frontier of AI and security, OpenSSF served as an advisor to DARPA's AI Cyber Challenge (AIxCC), which demonstrated that AI-driven systems can find and patch vulnerabilities in open source code at machine speed — with all finalist tools released as open source. OpenSSF brings a broad, cross-industry membership, a practitioner-driven governance model, and a track record of translating security challenges into shared, scalable solutions. We welcome engagement with policymakers to ensure that open source software remains a source of strength as well as secure, sustainable, and globally collaborative for digital infrastructure.

Additional Resources

1. Core Policy & Global Strategy

- https://openssf.org/public-policy/: Outlines the seven strategic pillars for government engagement, including public funding for security and international collaboration.
- https://openssf.org/resources/publications/secure-open-source-software-vision-brief-2025/: A high-level brief detailing the community's progress and future initiatives for securing digital infrastructure.

2. Regulatory Guidance (EU Cyber Resilience Act Focus)

- https://best.openssf.org/CRA-Brief-Guide-for-OSS-Developers: A practical guide for understanding how the EU's Cyber Resilience Act applies to open source projects.
- https://policy.openssf.org/CRA/stewards-playbook.html: A resource defining the roles of "stewards" versus "manufacturers" to help organizations navigate legal liabilities.
- https://openssf.org/blog/2026/03/02/case-study-defending-the-open-source-supply-chain-in-a-new-regulatory-era/: A detailed look at how community frameworks are being translated into scalable regulatory practices.
- https://training.linuxfoundation.org/express-learning/understanding-the-eu-cyber-resilience-act-cra-lfel1001/: An introductory educational offering designed for anyone needing a foundational understanding of the new law.

3. Security Frameworks & Security Baseline

- https://baseline.openssf.org/: A structured set of "minimum MUST" security requirements aligned with international standards like NIST and the CRA.
- https://slsa.dev/: A framework for ensuring the integrity of the software build process and protecting against tampering.
- https://securityscorecards.dev/: An automated tool that assesses a project's security health based on technical indicators.

4. Infrastructure & Repository Security

- https://repos.openssf.org/: The digital home for standards helping repository maintainers secure the distribution of software packages.
- https://repos.openssf.org/principles-for-package-repository-security: A maturity model establishing security tracks for authentication, authorization, and CLI tooling in package registries.
- https://openssf.org/blog/2026/02/19/advancing-package-repository-security-through-collaboration/: A summary of the Package Manager Security Forum's cross-ecosystem efforts to secure the global supply chain.
- https://repos.openssf.org/trusted-publishers-for-all-package-repositories: A technical framework for eliminating long-lived credentials in favor of short-lived, verifiable identity tokens.

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Thank you! Join us.

openssf.org/getinvolved

openssf.org