STIMSON

REPORT

Trade & Technology
Strategic Foresight Hub

Securing the Open Frontier: Voluntary Standards for Open-Source Security

By Giulia Neaher, Research Analyst, Strategic Foresight Hub, Stimson Center

October 2025

ABOUT STIMSON

The Stimson Center promotes international security and shared prosperity through applied research and independent analysis, global engagement, and policy innovation.

About the Authors

Giulia Neaher is a Research Analyst with the Strategic Foresight Hub at the Stimson Center, where she leads projects on AI and emerging technology policy. Prior to joining Stimson, Giulia served as Assistant Director at the Atlantic Council's GeoTech Center, where she led programming and authored research on responsible AI, international standards, and the geopolitical elements of technology. She also worked as a Research Associate at the Center for AI & Digital Policy, tracking U.S. AI policy developments and conducting advocacy for responsible AI. Giulia graduated with a Master in Public Policy from the Harvard Kennedy School, where she was a Public Service Fellow, and holds a B.A. in international relations and economics from Washington University in St. Louis.

Acknowledgments

This work originated as a master's thesis at Harvard Kennedy School – many thanks to Professor Jim Waldo, who advised on this paper and was an incredible resource and sounding board throughout. I am also grateful to the team at the Stimson Center that supported the continuation and publication of this work, particularly Julian Mueller-Kaler and Mat Burrows.

There are also many figures in the OSS space who spoke with me under Chatham House rule and who were integral to this paper. My heartfelt thanks go to the OSS, cybersecurity, and standards professionals who shared their time and expertise in interviews. I hope this work will sufficiently communicate your invaluable insights into the world of OSS.

Please Cite this Publication As

Giulia Neaher, 2025, *Securing the Open Frontier: Voluntary Standards for Open-Source Security*. The Stimson Center, Washington D.C., USA.

The Henry L. Stimson Center
1211 Connecticut Avenue NW,
8th Floor Washington, DC 20036
Tel: 202.223.5956 | Fax: 202.238.9604
www.stimson.org

October 2025

Securing the Open Frontier: Voluntary Standards for Open-Source Security

How can policymakers leverage voluntary standards to enhance cybersecurity in open-source software?

By Giulia Neaher, Research Analyst, Strategic Foresight Hub, Stimson Center

Open-source software (OSS) is key to much of the technology that powers modern life, making it a critical area of interest for cybersecurity policy. However, OSS governance demands creative thinking – though OSS is about as secure as commercial software, it can be difficult to govern through "traditional" regulatory measures. Rules that rely on firm structures for liability, accountability, and enforcement are a poor fit for the decentralized, volunteer-driven nature of OSS and the community that surrounds it. This paper explores how voluntary cybersecurity standards in OSS may offer a practical, ecosystem-specific pathway to strengthening OSS security and presents concrete policy recommendations for U.S. policymakers to support such standards effectively.

Contents

Executive Summary

Open-source software (OSS) is incorporated deeply into our digital ecosystem, across functions ranging from instant messaging to critical infrastructure. Though OSS is not necessarily riskier than commercial software, OSS security is critical given its prevalence in our rapidly changing digital environment and the complexity of implementing cybersecurity guidelines in the OSS space. The decentralized nature of OSS development and of the open-source community itself poses unique challenges to the uniform application of cybersecurity practices, which in turn makes regulation or other government engagement difficult.

This paper evaluates voluntary technical standards — here including widely adopted industry best practices as well as formal voluntary consensus standards developed by Standards Developing Organizations (SDOs) — as a potential mechanism for securing OSS. Voluntary standards are naturally suited to the decentralized nature of OSS and present a viable pathway forward for improving cybersecurity. Fourteen interviews with professionals in the open-source security and standards spaces reveal two key dynamics within OSS that impact standardization of OSS security: financial incentives and culture. Furthermore, interviewees identify the uptake of standards — as opposed to the design of standards — as a key inflection point that may benefit from formalized U.S. government support and put forth several policy suggestions.

U.S. policymakers interested in advancing the cybersecurity of OSS through standards should consider three policy recommendations identified in this paper: firstly, concerted government outreach to the OSS community; secondly, leveraging financial incentives to encourage cybersecurity; and thirdly, establishing government-managed repositories of standards to ease standards uptake.

Given the increasing role of OSS in powerful technologies like artificial intelligence (AI), it is critical that the government develop a clear strategy to enhance OSS cybersecurity. As technology becomes more capable, the ramifications of security incidents may become even more profound. To prevent or address such incidents, policymakers must develop interventions that are both effective and suited to the unique characteristics of the OSS space. This paper endeavors to inform policymakers about these unique characteristics and provide actionable pathways for future policy.

Introduction

In our digitized world, open-source software (OSS) has become ubiquitous, accounting for 80%-90% of all existing software.[1] OSS, loosely defined as software that is developed openly and collaboratively and is freely accessible for individuals to edit and download, is vital to key functions ranging from everyday texting to critical infrastructure. Part of the popularity of OSS is due to its accessibility and opportunity for innovation, but its decentralization can make cybersecurity difficult. In particular, conducting oversight, enforcing best practices for security, and determining liability in the event of a breach can be challenging in OSS. Moreover, recent developments such as the increasing popularity of open-source and open-weight large language models like Meta's Llama and hugely impactful cyberattacks like Log4Shell and SolarWinds highlight the need for improved security practices in OSS.[2]

How can policymakers support OSS security despite the difficulty of applying traditional, liability-driven forms of regulation? This paper will examine the utility of voluntary technical standards as a tool for enhancing the security of OSS and identify potential ways for the U.S. government to leverage standards in its cybersecurity efforts.

Acronyms

ANSI ..... American National Standards Institute

CRA ..... EU Cyber Resilience Act

ETSI ..... European Telecommunications Standards Institute

IEEE ..... Institute of Electrical and Electronics Engineers

IETF ..... Internet Engineering Task Force

ISO ..... International Organization for Standardization

ITU ..... International Telecommunications Union

LLM ..... Large-Language Model

OpenSSF ..... Open-Source Security Foundation

OSS ..... Open-Source Software

SDO ..... Standard Developing Organization

Background

Understanding the OSS Landscape

Any individual seeking to understand OSS governance must first realize that the OSS community is not a monolith. OSS exists in a complex ecosystem of interactions between hobbyists, nonprofit foundations, commercial operations, start-ups, and more. OSS projects range from those developed and maintained by just one person to large-scale software developed by hundreds of people working together. Some of the critical OSS utilized by the U.S. government or major commercial actors — such as OpenSSL, a widely used cryptography library — is run by just a few people.[3] Many OSS developers and maintainers work for free, but some are funded by major commercial software companies or academic institutions. In 2020, a survey by the Linux Foundation and Harvard University found that only 51.56% of OSS contributors are specifically paid to do so, and that the top three reasons people contribute to OSS are non-monetary.[4]

This paper will endeavor to make some sense of the many dynamics described above to evaluate the OSS landscape in relation to standards and cybersecurity.

Defining "Standards"

In conducting interviews for this paper, the first question from interviewees was often: "What do you mean by 'standards?'"

In general, "standards" is a broad term that can refer to any kind of guidance or technical specification. For this paper, however, "standards" is an umbrella term that can refer to any voluntary, widely known, and disseminated technical specification. In the OSS context, the two main examples of this type of standard are best practices and voluntary consensus standards developed by SDOs. These two types of standards represent the bulk of the standardization efforts within the OSS space, though their methods are very different.

Best practices are *de facto* standards that are adopted and determined by informal industry consensus. If practitioners find a certain methodology or tool maximizes functionality (or security, or efficiency, or another goal), it may evolve into a "best practice." Simply put, as OSS actors interact with and learn from each other, best practices emerge from the habits and processes that tend to work for most people. Though these standards are not codified, they have broad impact across the OSS space. *De facto*

standards can also become *de jure* — on some occasions, best practices are adopted and codified by SDOs.[5]

SAMPLE BEST PRACTICES

DevHunt, a website that hosts resources for OSS developers, lists the below as best practices for OSS security: [6]

- "Validate all user inputs and sanitize outputs.
- Use parameterized queries to prevent SQL injection.
- Implement role-based access control.
- Encrypt sensitive data.
- Adopt DevSecOps culture with security testing.
- Keep dependencies up to date.
- Configure infrastructure securely."

In contrast with best practices, voluntary consensus standards are *de jure*, approved through complex and formalized SDO processes. SDOs are nonprofit organizations that produce peer-reviewed technical standards for products across many sectors, but especially in the technology space. Examples of SDOs include the Institute of Electrical and Electronics Engineers (IEEE), the International Organization for Standardization (ISO), and the Internet Engineering Task Force (IETF). These SDOs also vary by scope, focus, and membership. For example, the IEEE allows both individuals and firms to join as members, while the International Telecommunications Union (ITU) also allows national representation.[7] The Internet Engineering Task Force (IETF) is known particularly for its work on the specific Internet protocol known as TCP/IP, while the European Telecommunications Standards Institute (ETSI) broadly leads on software standards for the European Union.[8]

Though the exact compositions of SDOs vary, SDOs generally rely on internal working groups consisting of volunteer technical experts, academics, and practitioners who evaluate proposals using criteria that include technical robustness, efficiency, cost, and user-friendliness. [9] Once selected, a standard is typically voluntarily adopted by the members of the SDO, and depending on the relevance and scope of an SDO's membership, SDO standards may quickly become industry norms. [10] There are no binding commitments for one member to adhere to a standard, but as outlined by the American National Standards Institute (ANSI), stakeholders often acknowledge that the system functions to the benefit of all in increasing interoperability between markets, reducing costs, and improving user experiences.[11] However, one key feature of SDO standards is that they often require a paid license through the relevant SDO, limiting their accessibility to those who are willing or able to pay.

OPEN STANDARDS

"Open standards" are widely available, free, and easily usable by OSS developers. There has been much discussion in the OSS space about the need for standards to meet this "open" designation to ensure that OSS developers are able to use standards as easily as commercial developers. Standards without an "open" designation, on the other hand, are often available via paid licenses.[12]

Working in parallel, best practices and voluntary consensus standards establish some uniformity in the open-source industry's technology and practices. However, adoption of such standards is not universal. As this paper will describe below, they are useful but imperfect tools for improving cybersecurity in the OSS space.

Table I: High-Profile Internet Standards

Standards are integral to the functioning of the Internet as we know it. The below examples are provided to illustrate how foundational standards are for our daily lives.

Standard	Description
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP) is the foundation of Internet communication. It comprises a suite of protocols that enable the delivery of messages between network-connected devices. TCP/IP enables all our digital conversations.[13]
HTTP (Hypertext Transfer Protocol)	HTTP is a protocol that enables data transfer between browsers and servers on the web, among other client-server relationships, acting as a crucial foundation for how we communicate online.[14] It is maintained by the IETF's HTTP Working Group.[15]

Security Incidents

Recent incidents in OSS have highlighted the need for improved security. Perhaps the most prominent of these incidents is the Log4Shell vulnerability, which was discovered in December 2021.[16] The vulnerability was located in the Apache Log4j library, a Java-based, open-source logging utility that was used widely by both the private sector and the U.S. government. Apache, the OSS foundation that maintains Log4j, rated the exploit as "critical" because it was relatively easy to harness, difficult to correct, and extremely widespread.[17] The vulnerability was particularly dangerous because it allowed for remote access and full control of affected systems.

Log4Shell was a zero-day vulnerability — a flaw that is unknown until the time of its discovery, at which point hackers can access it before the software vendor can correct the issue.[18] Apache was thus unable to resolve the issue before hacking occurred. This was a significant issue at the time because it was estimated that 10% of all digital assets were at risk due to Log4Shell.[19] To make matters worse, security assessments also reported that exploitation of Log4Shell would only increase after it became public.[20]

Unfortunately, Log4Shell was difficult to fix at scale. Apache immediately issued a patch, but earlier versions of the software present across the digital ecosystem had to be manually and individually corrected. Since Log4Shell is utilized in so many projects, even today it can be challenging for companies to ensure their own software is free of the issue, and even harder to screen all the third-party apps or services they use.[21] In 2022, Log4Shell was still among the most-exploited vulnerabilities in the world.[22]

After the Log4Shell incident, many leaders in government and industry alike became concerned about the security of OSS. Many feared that OSS was an ungoverned Wild West, inherently unsafe since anyone can contribute to software and view source code.[23] However, both OSS and commercial software can have breaches, and many in the OSS community have pushed back strongly against the belief that OSS is any less secure than commercial software.[24]

One commonly cited commercial software breach is the SolarWinds attack, a highly consequential breach that began in 2019 and had devastating effects on both government and society at large. In the attack, hackers accessed SolarWinds' proprietary software and injected malicious code into the software product Orion, an IT performance monitoring system. When SolarWinds released an update to Orion in 2020, the malware was then deployed to more than 18,000 customers. The backdoor created by the malware allowed hackers to access accounts and impersonate victims, including across multiple federal government agencies.[25] The attack is estimated to have cost the affected U.S. companies 14% of their annual revenue.[26] Estimates say that hackers — now believed to be a Russian group — may have had over a year of access to SolarWinds' systems through the breach before its discovery in December 2020, and that it may still be years before the full extent of their access and malicious input comes to light. [27]

Though OSS and commercial software can both be vulnerable to attack, OSS does feature some distinct characteristics that make cyber governance challenging. Some of the greatest assets of OSS can be problematic from a security perspective. For example, greater transparency can make it easier for bad actors to find vulnerabilities. In addition, since people with any level of programming or security knowledge can contribute to OSS, it can be difficult to ensure consistent quality and adherence to security standards across projects.[28] However, OSS also benefits from its collaborative nature; OSS projects are double- and triple-checked by many contributors, who are constantly on the lookout for errors and vulnerabilities.

Government's Role

Many federal agencies are involved in technology and cyber policy more broadly, including the White House Office of the National Cyber Director and Cybersecurity and Infrastructure Security Agency

(CISA). Congress has also been active in producing legislation related to open-source security. Some ongoing efforts are detailed below.

In the aftermath of the Log4Shell attack, the Senate Committee on Homeland Security and Governmental Affairs proposed a new piece of legislation titled the "Securing Open-Source Software Act," which instructed CISA, among other agencies, to take steps to improve OSS security.[29] The proposal did not pass, but it did receive widespread bipartisan support.[30] It details a pathway for the U.S. government to improve its understanding of the prevalence and use of OSS through risk assessments, and to subsequently accelerate the U.S. government's contribution to OSS itself and the OSS community more generally.

Moreover, CISA has recently undertaken significant actions to improve OSS security, some of which align with the goals outlined in the Act. For example, in September 2023, CISA published its Open-Source Software Security Roadmap, which sets goals for CISA's engagement in OSS security and outlines a plan to achieve them.[31] These goals include strengthening the relationship between CISA and the OSS community, raising awareness of OSS and associated risks, reducing OSS-related risks to the federal government, and generally improving the resilience and security of OSS.[32]

In 2021, the Biden administration produced an executive order focused on cybersecurity, which had a number of provisions impacting OSS. The section on supply chains, drafted in the wake of the SolarWinds attack, is particularly relevant for OSS deployment in government.[33] The order requires that federal agencies receive Software Bills of Materials (SBOMs), which formally document the supply chain for a given software product (including OSS elements), during software procurement from suppliers. NIST produced a standard for SBOMs to which these suppliers must adhere — this standard only strictly applies to federal suppliers but may be useful for others. [34] Mandated SBOM use in government means that vulnerabilities — whether in an OSS or commercial software product — will be easier to trace when incidents occur.

Related Efforts

This memo evaluates the intersection of OSS governance, security, and standards. There exist significant and meaningful bodies of work in those spaces, which are summarized briefly below.

Many publications related to **OSS governance** are academic or gray literature. These works often debate the complexity of governing OSS and evaluate potential avenues for regulation that gel with the unique structure of OSS. For example, a 2013 paper by De Noni, Ganzaroli, and Orsi performs an in-depth analysis of key dynamics and best practices in open-source governance. The paper dives deeply into OSS cultural values like creativity, independence, and innovation.[35] More recently, a paper drawn from the proceedings of the 2024 Association for Computing Machinery *Conference on Human Factors in Computing Systems* evaluated formal governance systems in OSS.[36] Outside of academic literature, OSS foundations produce shorter articles or applied guidance related to OSS governance.[37]

Meanwhile, much of the existing activity in **OSS security** comprises government recommendations (like CISA's OSS Security Roadmap), short-form blogs, and programming from OSS foundations. For example, the Open-Source Security Foundation (OpenSSF) hosts and creates resources for OSS developers and maintainers to improve security, publishes opinion pieces related to trends in OSS security, and coordinates public policy efforts, among other activities.[38] Just as individual actors play an important role in OSS itself, important community figures also publish regularly about OSS security trends and practices in publications like TechRepublic.[39]

The literature on **voluntary standards in OSS** mostly analyzes the ways in which SDOs engage with the OSS space. For example, in 2017, the European Commission collaborated on a report with Open Forum Europe that outlined a plan for SDOs to build better relationships with OSS. [40] Not all reports, however, favor increased collaboration between OSS communities and SDOs. A widely cited 2020 report by Michele Herman suggested that SDOs reduce their reliance on licenses produced by the Open-Source Initiative (OSI) when producing OSS projects in-house.[41] Herman argues that the very openness and accessibility of OSS licenses can be antithetical to the goals of SDOs, which seek uniformity and strict conformity to standards.[42]

Information about **best practices for OSS security** is also plentiful, though scattered across the ecosystem. Many individuals, organizations, governments, and OSS platforms list security best practices: For example, OpenSSF hosts an inventory of security best practices on GitHub,[43] and blog posts on the subject are abundant.[44,45]

This memo draws on the aforementioned bodies of work to provide a backdrop for the interviews that drive its policy recommendations. Research and programming about OSS governance, security, standards, and best practices all provided the bases for interviewee and question selection, which is outlined in the Methodology section.

Methodology

This paper draws primarily upon fourteen interviews with experts across the OSS ecosystem. The list of interviewees represents a variety of professional roles and areas of expertise, and it includes:

- OSS developers and maintainers
- Think-tank and academic researchers working on open-source security and related issues
- SDO representatives
- Major OSS foundation representatives
- Past and current government experts from agencies and departments, including the Department of Defense, CISA, the National Institute of Standards and Technology (NIST), and the National Science Foundation (NSF)
- Cybersecurity professionals

The study comprised semi-structured interviews, lasting approximately 45 minutes each and conducted between December 2024 and March 2025. The interview protocol included questions related to:

- The utility of standards for increasing cybersecurity of OSS
- The nature of interactions between the variety of stakeholders in the OSS ecosystem (including large OSS foundations, individual OSS developers, small OSS companies, commercial operations, SDOs, and government bodies)
- Relationships between the U.S. government and OSS actors
- Barriers to adoption of OSS security standards
- The development process of OSS security standards
- Perspectives on potential policy interventions

While this research represented a broad range of expert perspectives, it did have key limitations. Firstly, the sample size of fourteen experts can hardly represent the whole of the OSS security and standards ecosystem, which, as mentioned, is complex and varied. Secondly, the rapid speed of technological development and regulatory change in recent months could mean that by the time of publication, certain suggestions or findings may no longer be relevant or sufficient.

Appendices I and II contain more detail on interview questions and interviewee backgrounds.

Findings

This memo classifies interview findings into three categories. Firstly, interviewees identified some dynamics — here called Key Characteristics of OSS — that shape the OSS security space. Secondly, they identified two Key Metrics for Standards that determine the efficacy of standards. Thirdly, they proposed several Policy Options that may be ripe for federal or congressional engagement. The Findings section summarizes all interviews broadly, but some statements cite particular interviews.

Key Characteristics of OSS

Interviewees identified several drivers that shape the role of standards in the OSS security space. The two elements that were mentioned most frequently are finances and culture, both of which are highly influential in determining OSS community priorities, incentives, and views on policy proposals.

I. FINANCES

The heterogeneity of the OSS landscape means different actors may have widely diverging financial incentives. For some programmers and maintainers, there is no financial incentive at all, as many OSS contributors work for free, driven by creativity and a passion for software. These may be individual hobbyists working on personal projects or small volunteer teams working to develop OSS tools. On the other hand, many large technology companies and nonprofit OSS foundations pay for their employees to contribute to OSS development and maintenance. Though OSS itself does not directly produce profits, since the software is free, the private sector recognizes how foundational OSS is to the functioning of the Internet. By contributing code to the OSS space, companies can help shape key OSS projects that are useful to their businesses and later benefit from community contributions to said projects.[46] However, it is important to note that OSS maintainers and developers paid by large companies are often people who previously worked for free on valuable OSS projects and were funded to continue that work. Accordingly, corporate funding of OSS work does not correspond to any ownership or control of the projects in question.

All interviewees reported that individuals working on a volunteer basis are less likely to seek out and implement technical standards —not out of a lack of care for the quality of their outputs, but because of the simple fact that they are already working for free. Oftentimes, seeking out standards, learning how to use them, and then implementing them adds to developers' workloads significantly, and there is little incentive for unpaid developers to do extra work they do not enjoy.

> ***Anytime you're asking an upstream project or developer to do unplanned, and from their perspective, low value, work... It is a challenging prospect and requires a lot of interpersonal and community skills to be able to persuade them to your case. – Interview with Anonymous American OSS Foundation Staffer, 2/19/25***

On the other hand, larger OSS projects run by foundations and corporations tend to more regularly incorporate standards, largely due to structural factors. When individuals are employees of a large software company that adheres internally to certain best practices or industry standards, they may default to utilizing standards in their OSS work, creating a sort of trickle-down effect.[47] Moreover, when working on large OSS projects, uniform use of standards is likely to be useful in ensuring the structural integrity of the project as a whole and in ensuring the interoperability of the OSS project with other software or hardware.[48]

II. CULTURE

> ***Yes, there's one open-source community. But there's lots of mini communities within that one community, right? And they all have different motives. They all have different reasons for being there. – Interview with American University Professor, 2/11/25***

The culture of OSS is also highly relevant to the role of standards. As mentioned above, the OSS community is anything but monolithic; just as financial incentives vary, so do individual goals, priorities, and attitudes. Nonetheless, some broad themes are visible. Open-source culture can in many ways be compared to that of the early Internet: collaborative, decentralized, and innovative.[49] According to all interviewees, the community places a high premium on independence, favoring practices and norms that allow individuals to operate without constraints to maximize innovation. Relationships in the OSS community do not reflect traditional hierarchy or static leadership structures. Rather than bestow titles or roles, the OSS community relies heavily on individual reputation and interpersonal trust.

This emphasis on independence can also translate to resistance to anything viewed as excessive oversight or centralization of power. For many in the OSS community, such activity would run counter to the very nature of open source; many fear that if their activities become highly limited by regulation, the spirit of creativity and collaboration that define OSS would vanish.[50] The worst-case scenario for such individuals is one in which OSS ceases to be freely accessible by developers of all shapes and kinds.[51]

> ***The free and open culture, and the fact that all of our projects are publicly available, that's kind of the core ethos. The code must be visible. It must be downloadable, editable... and that means you're inviting anyone, from anywhere. – Interview with American OSS Foundation Staffer, 2/19/25***

Moreover, the fact that many OSS contributors work for free and contribute to OSS as a hobby or passion project means that any policy actions will require voluntary buy-in from the community. In

part, traditional regulation does not work for OSS because it is difficult to tell someone how to do work they do for free. What does mandating the use of security standards mean to an unpaid contributor working on a passion project? Even if the contributor were barred from working with OSS foundations or on usual OSS platforms, they could still code or contribute to alternative projects in their spare time.

When interacting with the open-source community, therefore, it is vital that government actors do so with respect for independence and innovation. Any policy actions must consider the need to avoid centralization of power or onerous regulations, which would alienate community members. OSS is built upon the contributions of that community; the loss of trust or interest in OSS from its contributors would be devastating. Moreover, it is crucial for policymakers and agencies to cultivate a reputation for both technical expertise and trustworthiness. If the OSS community does not trust U.S. government representatives, it will be far less likely to take up federal recommendations or engage in programming.

Key Metrics for Standards

Interviewees also identified two axes that can be used to evaluate security standards for OSS: firstly, the technical adequacy of standards, and secondly, the uptake of standards. Do standards generally represent the most efficient, cost-effective, and technically sensible path forward for developers and users? And even if they do, are the standards actually being used? Even if a standard meets all technical criteria and its implementation meaningfully improves OSS security, the standard is useless until it achieves community adoption.

1. TECHNICAL ADEQUACY OF STANDARDS

Overwhelmingly, interviewees agreed that the technical sufficiency of standards is high; none of the interviewees noted any concerns with the technical effectiveness of standards in the current OSS security environment.

SDOs select standards based on a combination of factors that aim to evaluate overall effectiveness. These may include technical excellency, resource efficiency, consensus, and cost-effectiveness.[52] SDO working groups comprise technical experts from academia and industry, and members tend to have a strong understanding of which software practices will be the most effective and feasible.

Best practices are also quite technically sound. By their nature, best practices are selected by practitioners on the basis of their performance. Anything that is ineffective or unsuitable will not be adopted by community members.

2. UPTAKE OF STANDARDS

The uptake of standards, however, is far more complex. As outlined above, there is often little incentive for OSS developers to adopt and implement standards into their work. Beyond the cultural and financial mismatches outlined above, other challenges affect the uptake of standards:

- **Paywalls and licensing for SDO standards.** As mentioned above, oftentimes formal SDO standards are accessible only via paid licenses.[53] For most developers working for free, paying to access a standard is out of the question. Moreover, paid licensing for SDO standards can be a point of moral objection for OSS developers, who are committed to fostering a free, open, and collaborative software ecosystem.[54] OSS developers are often even unwilling to submit their own projects for consideration as standards by SDOs if that means their work will become accessible only via paid license. In the past, OSS developers who have submitted their own work as standards have later found that they themselves are required to pay to license their own software.[55] Paid licensing for standards, in other words, is both a cultural and a financial mismatch for the OSS community.

- **Difficulty of locating standards.** Even when SDO standards and best practices are freely available, it can be difficult for developers to identify which standards they should use and how. Different OSS projects have different security needs and applicable standards, and hobbyists or developers working on smaller-scale projects may not always have knowledge of which standards are appropriate. Many standards are shared through OSS foundations like Linux and on community boards on GitHub or Reddit, but there is no single repository for the use of technical standards or best practices. This further adds to the complexity of integrating security standards into an already-decentralized OSS ecosystem.

- **Cost and difficulty of retrofitting OSS software.** Even when OSS standards are readily available, and developers know which ones to use, they still face a significant hurdle: implementation. As described above, most standards are technically sensible and useful, and they can be utilized in the development process of a new project with some additional time and effort. However, the adoption of new standards is particularly challenging in the context of already-extant OSS projects. Large OSS projects with many collaborators are particularly hard to update, as anyone seeking to update such a project would need to go into the complex web of code and understand how it works in depth before even beginning the update process. This takes a large amount of time and energy, which once again runs into the problem of incentives.

THE CRA AND INTERNET BALKANIZATION

A development in the European Union may also impact global uptake of OSS standards. The Cyber Resilience Act (CRA), which entered into force on December 11, 2024, promotes cybersecurity for software and hardware with digital elements. When the bill was being developed, some OSS community members raised the alarm about a possible balkanization of OSS; currently, the OSS space is highly international, and the imposition of different regulations across jurisdictions could split that space by physical geography.[56] As a result, the CRA as it was passed avoids burdening OSS. For example, OSS developers are not liable for their projects if they are not for sale. If the software is used as an element of a product that is sold on the market, liability falls on the company that sells the derivative product.

Moreover, in lieu of mandating OSS security practices, the CRA created "open-source stewards" that will assume responsibility for the security of OSS.[57] Post-CRA efforts to regulate OSS should consider the risk of balkanization as well as potential pushback from the OSS community.

Policy Options

Given the above constraints, interviewees identified several potential mechanisms for the improvement of security standards in OSS. These suggestions focus on increasing uptake, not technical efficacy, since interviewees did not believe any change to the latter to be necessary.

I. ALIGNING FINANCIAL INCENTIVES

This analysis has established that financial incentives are key in the adoption of security standards. One interviewee raised the possibility of paying larger OSS actors with full-time employees — such as foundations or contributing commercial companies — to rewrite complex OSS projects in accordance with federal guidance on memory safety or other cybersecurity goals. Five interviewees independently echoed or responded enthusiastically to this idea, and none objected. Some work is already being done in this space, at a smaller scale. For example, GitHub funds individual maintainers to join three-week OSS security sprints that aim to find and remediate vulnerabilities via its Secure Open Source Fund.[58]

MEMORY SAFETY

One of CISA's recent priorities has been the "memory safety" of software.[59] The ways in which programs access memory locations can sometimes leave them vulnerable to errors that provide entry points for bad actors. Certain coding languages, specifically C and C++, are more susceptible to these types of errors. CISA therefore encourages using languages that are more robust with respect to memory safety. In late 2024, CISA and the FBI jointly stated that software companies should abandon C and C++ by January 1, 2026, in order to comply with (voluntary) memory safety guidelines.[60] Rust, another coding language, is the gold standard for this function, and CISA strongly encourages its use within government and in general.

It takes a huge amount of time, manpower, and money to rewrite and redesign programs from C or C++ into Rust. The process is not as simple as translation between languages; coding languages are not exact analogues of one another, and switching often requires the deconstruction of a project down to

its smallest pieces in the original language and subsequent reconstruction in an entirely new structure in the new language. Large enterprises and foundations have the necessary structure and manpower to update these projects, but they will require a strong incentive to do so. This incentive could be financial, as the interviewee suggested; however, another interviewee noted that it may be difficult to sway multibillion-dollar technology companies with a government grant alone.

II. CREDENTIALING

Another interviewee raised the possibility of requiring OSS developers and maintainers to obtain formal credentials signaling their technical capabilities and knowledge of security standards. Moreover, they suggested that developers be required to input and verify said credentials to contribute to OSS projects. This system would ensure that OSS contributors possessed adequate technical skills and knowledge of security practices, thereby boosting the security and quality of OSS projects.

However, this concept was unpopular amongst other interviewees. They feared that mandatory credentialing would exclude certain developers from participating in OSS, contradicting the core tenet of OSS (namely, that anyone can contribute). Credentialing has already been proposed in the OSS space, and the idea has been widely rejected by OSS community members.

III. BADGING

An alternative to credentialing for individuals is credentialing for *projects*. In this proposal, projects that meet certain standards (security or other) become eligible to receive public "badges." These badges signal a project's quality to OSS community members and to users interested in downloading or otherwise utilizing the software project. Badging is already in practice in the OSS space. Four interviewees, for instance, noted OpenSSF's Best Practices Badge, which is available to projects meeting a certain set of security criteria.[61]

Interviewees viewed badging very differently from the credentialing described in Option II. Badging serves only to signal a project's quality — it does not limit or preclude anyone wishing to contribute to it. Moreover, since individual reputation is often important to OSS developers, the opportunity to contribute to a badged project can be attractive to community members.

IV. RESOURCE ACCESSIBILITY

All interviewees in one way or another highlighted the complexity of accessing and utilizing standards. Since there is so little incentive for individuals to independently take up standards, any barrier to access can be significant. Many developers are unlikely to go out of their way to search for appropriate standards, especially if such a search takes significant time or effort. One early interviewee suggested that creating a centralized, searchable database for OSS standards could help to reduce such barriers, and all subsequent interviewees responded favorably when presented with the idea.[62]

V. COMMUNITY ENGAGEMENT

Four interviewees independently noted that CISA's recent engagement in the OSS space has been successful in building trust with OSS community members and developing a reputation for CISA as a neutral and worthy partner. In particular, they mentioned the recent hiring of OSS practitioners with deep knowledge of the space and CISA's Spring 2024 workshops with community members.[63] Interviewees noted that continuing such engagement would help to lend weight and credence to suggestions when it comes to OSS security.

VI. CASE STUDIES

One interviewee suggested that it may be useful to investigate certain successful OSS standards as case studies. As mentioned above, some of the most powerful OSS standards are those that began as de facto best practices and were later codified by SDOs. Such standards have the approval of OSS practitioners, who choose to adopt them as useful best practices, and they reach a critical mass such that it becomes logical to formally codify them. Why do some standards achieve this widespread uptake in the OSS community, and not others? Further research into successful cases may prove instructive for the U.S. government's future OSS policies.

Evaluation Criteria

The characteristics, metrics, and policy options above can be synthesized into a set of evaluation criteria for policy recommendations. That is, any policy actions undertaken by policymakers should be justifiable and impactful according to the specifications and needs outlined above by the interviewees.

Each criterion was taken from interviewees' insights and is evaluated on a scale from 1-5, with 1 indicating poor alignment and 5 indicating excellent alignment. Each policy option can be assigned a total score out of 15 points, since there are three core criteria worth five points each. These evaluation criteria and corresponding metrics are described in further detail in the Appendix.

CRITERIA INCLUDE:

1. Positive OSS Community Response

For any voluntary standard to succeed in increasing cybersecurity of OSS, community stakeholders must *choose* to employ it. OSS relies on voluntary contributions from its community members, who could cease said efforts or simply ignore suggested standards if they do not feel them to be reasonable. A low score on this metric indicates a hostile response from the community, and a high score indicates a positive and welcoming response.

2. Ease of Implementation

When considering policy options, the feasibility of implementation by the U.S. government is a key consideration; many policy ideas may sound impressive but be difficult to actually execute. A low score on this metric indicates a high degree of difficulty in implementing the policy, whether due to cost or regulatory hurdles, while a high score indicates that the policy has a well-established or easily accessible pathway to implementation.

3. Impact on Standards Uptake

The most important criterion here is the achievement of the desired effect: namely, an increase in the uptake of voluntary standards that enhances the cybersecurity of OSS writ large. A low score indicates a likely negative or negligible effect on OSS security, while a high score indicates a likely significant positive effect.

Policy Option Analysis

Each policy option identified by the interviewees was then evaluated along the aforementioned criteria, with the following findings:

EVALUATION OF OPTION 1: FINANCIAL INCENTIVES

Score: 12/15 possible points

This option is likely to receive a strong positive response and have a significant effect on OSS security. However, the likely costs and administrative hurdles involved in implementation slightly diminish its score, along with the fact that individual contributors and smaller outfits would likely be left out of such funding schemes, further entrenching funding disparities in the community.

EVALUATION OF OPTION 2: CREDENTIALING

Score: 5/15 possible points

This option is likely to receive a strong negative response and incur significant technical and financial hurdles. While it could have a strong impact on security for compliant individuals, the high probability of a decrease in OSS development overall would likely neutralize any positive impacts.

EVALUATION OF OPTION 3: BADGING

Score: 12/15 possible points

This option has already received a positive response in the community, and it is quite feasible from a technical perspective. Small hurdles would be posed by staffing and programmatic costs on the USG side and by the fact that individuals without an interest in reputation-building would likely be unaffected or uninterested.

EVALUATION OF OPTION 4: RESOURCE ACCESSIBILITY

Score: 11/15 possible points

This option would likely receive a strong positive response, and it would positively benefit the ease of

standards uptake. However, its principal challenge lies in implementation, which would likely require the development of dedicated infrastructure within a federal agency.

EVALUATION OF OPTION 5: COMMUNITY ENGAGEMENT

Score: 13/15 possible points

This option is strong across criteria, with a likely synergy of positive reactions, feasibility, and impact. Some challenges are posed by the need for a sustained hiring initiative and time investment.

EVALUATION OF OPTION 6: CASE STUDIES

Score: 10/15 possible points

This option is likely to achieve a positive response, but feasibility and impact face some uncertainties related to funding, staffing, and the eventual lessons drawn from the selected case studies.

These evaluations are further elaborated in table format in Appendix IV.

Recommendations

Four of these suggestions achieve a score greater than 10/15 possible points, and thus, appear to be effective in maximizing results along the selection criteria: badging, community engagement, financial incentives, and resource accessibility. The latter three of these will be the final recommendations of this memo, and a note on badging is included below.

A NOTE ON BADGING

The evaluations above also highlight the issuance of security badges as a highly feasible and impactful option. However, badging will not be included as a recommendation in this memo because other leaders in the open-source space (notably OpenSSF) are already successfully implementing this practice. An intervention in this area would likely duplicate efforts that are already underway. If policymakers desire to engage in OSS badging without directly creating or implementing badges, they can choose to promote the use of existing badges and support similar community endeavors.

Recommendation 1 – Community Center: Government as a Convener

Recommendation 1 can be highly beneficial in empowering the U.S. government to make positive contributions to the OSS community. By continuing to build trust between government and OSS practitioners, policymakers increase the likelihood that their recommendations and guidelines will be taken seriously. This option is highly feasible and likely to be very impactful.

A selected federal agency could build relationships in the OSS community by hiring open-source experts as full-time staff and hosting more community-building sessions. Multiple interviewees highlighted the efficacy of hiring seasoned open-source professionals in building trust within the community since these individuals bring their personal networks and reputations to government. As mentioned above, the OSS space relies on reputation rather than hierarchy, and if prominent OSS professionals express trust in government by joining as staff, the federal government's own reputation will benefit accordingly.

Interviewees also highlighted the working sessions held by CISA's OSS staff last year. These working sessions have the dual benefit of increasing security collaboration within the OSS community and building personal relationships between government staff and prominent OSS practitioners.

To implement this recommendation, a selected federal agency, such as CISA or NIST, should hire OSS professionals as full-time staff to a dedicated Open-Source Security team. This is highly feasible, given previous activity in this space. Moreover, this action would also make Recommendations 2 and 3 much easier by introducing more dedicated staffers to execute OSS projects. Of course, this implementation may be complicated by the costs of staffing and developing the necessary organizational infrastructure.

Recommendation 2 – Money Talks: Leverage Financial Incentives

The evaluation table above shows that the use of financial incentives is likely to be well-received and impactful. The involvement of significant federal funding is likely to be the greatest hurdle to this option.

Policymakers should consider developing a financial incentives program to encourage the adoption of OSS security standards. Interviewees said that large commercial enterprises and foundations have the manpower to take on the rewriting of OSS projects in accordance with security standards, but that they may lack the incentives. Financial incentives may be interesting to commercial enterprises, but they would likely need to be very large to appeal to major companies with large numbers of employees.[64] Incentives are more likely to be meaningful in the case of large OSS foundations like Linux, Apache, or Eclipse, which usually operate as nonprofits.

An agency like CISA or the Department of Commerce could create an OSS Security Grants Program, which would provide large financial grants to OSS foundations with the stipulation that they be used to rewrite important OSS projects according to security standards. The grant maker could issue a Request for Proposals (RFP) to assess potential grantees. The administrative burden would involve the identification of key OSS projects that need rewriting, the design and review of RFPs, the distribution of funding, and monitoring and evaluation of grantees.

Such a grants program could be hosted under the existing Open-Source Security umbrella, and it could be administered by existing program staff. If the U.S. chooses to expand the staffing of dedicated staff for OSS, as outlined in Recommendation 1, these employees could be tasked with designing and administrating the grants program.

The greatest challenge to this project is likely to be funding; in order for awards to be meaningful to large open-source organizations (even nonprofit foundations), the amounts would need to be significant to account for the time and manpower required by this effort. To address this issue, interested policymakers should produce an initial, detailed proposal for this project with a budgetary analysis.

Recommendation 3 – Standards for All: Increase Accessibility

Another feasible policy option is to create a federally managed database of technical standards, available to OSS developers free of charge. This option is precedented, feasible, and likely to be impactful.

By providing a free, easily navigable resource for the identification and implementation of standards, government can significantly reduce the burden on OSS developers. Though this approach does not necessarily introduce a new incentive, it does reduce barriers to standards uptake. Program leads could also choose to collaborate with existing OSS leaders or platforms to integrate this database and search function into common OSS tools. For example, this resource could be integrated into GitHub, which already hosts some centralized security guidelines for developers.[65]

This project would need to be split into two phases. Phase 1 would be initial development, and Phase 2 would involve long-term updating and maintenance. Phase 1 would be the most time- and resource-intensive. A federal agency would need to dedicate a team, comprising Open-Source Security staff or external contractors, to the creation of the database. Contractors require a fee, and internal staff would need to bill significant hours to this project. In Phase 2, once the database and search tool are created, the project will only require some ongoing maintenance, which can be managed with much less staffing and resource expenditure. The long-term maintenance of the program could be led by one or two Open-Source Security staffers as part of their routine activities.

The greatest uncertainties for the implementation of this project are the funding and staffing of Phase 1; as in Recommendation 1, a government agency or team responsible for the effort would need to be selected, and new funding would need to be allocated for the development and maintenance of the effort in the long-term.

Key Takeaways

- The OSS community is **not a monolith**. The community comprises individuals, groups, hobbyists, professionals, foundations, and companies.
- There are **differing incentives** for different actors in the OSS space.
- Understanding the **culture of OSS** is critical to effective policy engagement. Reducing the freedom of OSS actors to innovate and collaborate harms the very fabric of OSS and could significantly reduce software output and quality.
- Standards work well from a technical standpoint. Policymakers should aim to increase the **uptake of standards**, not redesign them.
- There are many ways that the federal government could engage with OSS standards to improve security, but three viable recommendations are **1) building strong relationships with the OSS community, 2) introducing financial incentives, and 3) increasing access to standards.**

The Path Ahead

Open-source software is the foundation of some of the most valuable and widely used programs in the world. Its contributions to modern society and software infrastructure are enormous, and the community of developers and maintainers that keep it alive perform a critical function for all of us. A 2024 Harvard Business School report found that the supply-side value of OSS is $4.15 billion, and that its demand-side value is $8.8 trillion, meaning that OSS provides a huge amount of value to the global economy relative to its development costs.[66]

However, by its very nature, OSS is difficult to govern. Since contributions to OSS development are so widely distributed, it is impossible to apply traditional, binding measures of regulation that rely on the assignment of liability. Voluntary standards avoid this problem, but it is inherently difficult to ensure the widespread uptake of voluntary measures. The federal government can improve uptake by providing financial incentives, increasing the ease of access to standards, and maintaining ongoing dialogue with OSS practitioners.

OSS is a key part of our digital environment and our increasingly digital lives, and our government has the power and opportunity to leverage voluntary standards to make OSS more secure for us all. This work is vital to the cybersecurity of U.S. critical infrastructure. It will help to prevent and address future OSS vulnerabilities affecting our national security, like the Log4Shell attack. It also may provide valuable lessons as open-source and open-weight AI become more common. Ultimately, lessons from the application of standards for OSS security may prove to be instructive in governing the open-sourced technologies of the future.

Appendices

Appendix I:
Interview Questions

Appendix II:
Broad Interviewee Descriptions

Appendix III:
Evaluation Criteria

Appendix IV:
Evaluation Matrix

Appendix I. Interview Questions

As mentioned in the *Methodology* section, this paper draws on 14 45-minute semi-structured interviews. Exact questions varied depending on the interviewee, but some sample questions are listed below:

1. Can you talk a little about how standards are used in OSS security?
2. How does the culture of OSS shape interactions with standards?
3. Can you think of any ways in which the standardization system itself may be altered to improve security?
4. Are there any specific areas of improvement for the use of standards in OSS security? Do you have any particular policy suggestions or solutions in mind?
5. How would you describe the federal government's role in the OSS community?

Appendix II. Broad Interviewee Descriptions

Interviews are organized by date. All are anonymized and non-attributable.

1. Interview with American Computer Scientist - 12/13/24
2. Interview with Former U.S. Federal Government Official - 1/30/25
3. Interview with American University Researcher - 2/6/25
4. Interview with American Congressional Staffer - 2/7/25
5. Interview with American University Professor - 2/11/25
6. Interview with American Cybersecurity Professional - 2/12/25
7. Interview with American OSS Community Leader - 2/12/25
8. Interview with American SDO Staffer - 2/12/25
9. Interview with American OSS Foundation Staffer - 2/19/25
10. Interview with American Cybersecurity Professor - 2/20/25
11. Interview with U.S. Federal Government Official - 2/20/25
12. Interview with European OSS Community Leader - 2/25/25
13. Interview with Former U.S. Federal Government Official - 2/26/25
14. Interview with European OSS Foundation Staffer - 3/12/25

Appendix III. Evaluation Criteria

I. POSITIVE OSS COMMUNITY RESPONSE

(1) Strong Negative	(2) Negative	(3) Neutral	(4) Positive	(5) Strong Positive
Antagonistic; policy action will be impossible.	Moderately antagonistic; policy action may be possible in a limited capacity.	No support or hostility towards policy action.	Some community support for policy action. May add reputational value for government in the OSS space.	Strong community support and engagement. Adds reputational value for government in the OSS space.

II. EASE OF IMPLEMENTATION

Very Difficult	Difficult	Possible	Easy	Very Easy
Requires significant work and funding. Requires Congressional appropriations. Long wait to see results.	Requires a higher operational burden and additional funding. Likely need for Congressional appropriations. Long wait to see results.	Some additional funding or staffing needed. Possible need for Congressional appropriations. Medium wait to see results.	Implementation aligns with current workstreams; little additional staffing or funding needed. Short-to medium wait to see results.	Implementation structure or process already exists; little or no additional staffing or funding needed. Shows results in the short term.

III. IMPACT ON STANDARDS UPTAKE

Negative	None or Mixed	Low Positive	Positive	High Positive
Actively reduces standards uptake.	Has no impact, or some components have a positive impact while others have a negative impact.	Somewhat increases uptake of standards in the short term or has potential to increase it in the long term.	Increases uptake demonstrably in the short term.	Increases uptake demonstrably in the short term and long term.

APPENDIX IV. EVALUATION MATRIX

	1 – Response	2 – Feasibility	3 – Impact
Financial Incentives (12/15)	Positive response from grantees; incentivizes good behavior without punishing anyone or imposing restrictions. **Positive (4)**	Necessitates the development of a process to bid for grants, evaluation criteria, etc. Also requires appropriation of significant federal funds. Development process may be time-consuming, but effects will become evident quickly once projects are launched. **Possible (3)**	Facilitates implementation of memory safety and other standards in large-scale OSS projects. Impactful in the short term and at a potentially large scale. **High Positive (5)**
Credentialing (5/15)	Widespread negative response. Viewed as imposing restrictions on who can contribute to OSS, which runs counter to core beliefs. **Strong Negative (1)**	Requires the development of training programs. OSS infrastructure would need to be rewired to make access credentials necessary to contribute to OSS. Development and rollout would both take a significant amount of time. **Very Difficult (1)**	Would make standards uptake a requirement, drastically increasing the use of standards. However, many OSS contributors would likely stop engaging in the space, greatly diminishing OSS output overall. **Mixed (3)**
Badging (12/15)	Positive response from OSS contributors, who welcome the opportunity to build reputational cachet by attaining badges. Does not exclude anyone from OSS and thus aligns with core beliefs. **Positive (4)**	OSS foundations are already working in this space. USG could choose to support their ongoing work or develop its own badges, modeled after those that exist in the field. Can be acted upon immediately or in the short term. **Easy/Possible (4)**	Would incentivize standards uptake for individuals interested in building a reputation in OSS or contributing to widely utilized projects. Individuals who do not share these interests would be unaffected. **Positive (4)**

	1 – Response	2 – Feasibility	3 – Impact
Resource Accessibility (11/15)	Positive response from OSS community. CISA's work to record cyber vulnerabilities has been widely utilized by cybersecurity professionals, who appreciate access to useful resources. Nonexclusive and thus aligned with core beliefs. **Positive (4)**	Requires a team to compile standards and build a search tool. May require appropriation of minor additional funds and specific staffing for the management of this program within a federal OSS team. Development will take time, but effects should be quick once the tool is rolled out. **Possible (3)**	Would make it easier for interested developers to access standards. Lowering barriers to access may reduce the disincentives for unpaid developers to seek standards resources. **Positive (4)**
Community Engagement (13/15)	Strong positive response from OSS community, as reflected in interviews. **Strong Positive (5)**	Requires the hiring of staff with strong ties to the OSS community —ideally career staff that can build long-term relationships. Requires sustained time investment but may show results quickly. **Possible (3)**	Would build trust with the OSS community, lending weight to USG's suggestions about OSS security and gaining allies to support the adoption of certain standards or practices. **High Positive (5)**
Case Studies (10/15)	Likely positive response. Does not restrict any OSS activities, and since it will highlight positive use cases, it may provide reputational advantages to involved developers. **Positive (4)**	Requires a dedicated research pipeline, complete with staffing and likely funding. Can be led by federal OSS staff, if present. Likely to take a long time to complete the research, and significant further time investment will be needed to create actionable policies based on findings. **Possible (3)**	Would provide deeper insights into what drives the uptake of standards. Subsequent policies could draw on these insights. Potential for great impact or little impact, depending on findings. **Low Positive (3)**

Bibliography

ANSI. "What Is ANSI?" Accessed March 30, 2025. https://share.ansi.org/Shared%20Documents/News%20and%20Publications/Brochures/WhatIsANSI_brochure.pdf.

Bekkers, Rudi, and Dongback Seo. "(PDF) Importance and Comparison of Standard Development Organizations in the Ubiquitous Society," January 2008. https://www.researchgate.net/publication/255579802_Importance_and_comparison_of_standard_development_organizations_in_the_ubiquitous_society.

Bera, Rajeev. "Strengthening Open Source Software: Best Practices for Enhanced Security – Open Source Security Foundation." OpenSSF, n.d. https://openssf.org/blog/2023/09/06/strengthening-open-source-software-best-practices-for-enhanced-security/.

Black, Paul E, Barbara Guttman, and Vadim Okun. "Guidelines on Minimum Standards for Developer Verification of Software." Gaithersburg, MD: National Institute of Standards and Technology (U.S.), October 6, 2021. https://doi.org/10.6028/NIST.IR.8397.

Boehm, Mirko. "The Relationship Between Open Source Software and Standard Setting." Creative Destruction & Me, November 14, 2019. https://www.creative-destruction.org/publication/ec-jrc-oss-sdo/.

Bradbury, Danny. "When Software Depends on a Project Thanklessly Maintained by a Random Guy in Nebraska, Is Open Source Sustainable?," May 10, 2021. https://www.theregister.com/2021/05/10/untangling_open_sources_sustainability_problem/.

Chakraborti, Mahasweta, Curtis Atkisson, Ştefan Stănciulescu, Vladimir Filkov, and Seth Frey. "Do We Run How We Say We Run? Formalization and Practice of Governance in OSS Communities." In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 1–26. CHI '24. New York, NY, USA: Association for Computing Machinery, 2024. https://doi.org/10.1145/3613904.3641980.

CISA. "CISA Open Source Software Security Roadmap," September 12, 2023. https://www.cisa.gov/resources-tools/resources/cisa-open-source-software-security-roadmap.

CISA.gov. "2022 Top Routinely Exploited Vulnerabilities," August 3, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a.

CISA.gov. "CISA Announces New Efforts to Help Secure Open Source Ecosystem," March 7, 2024. https://www.cisa.gov/news-events/news/cisa-announces-new-efforts-help-secure-open-source-ecosystem.

CISA.gov. "Mitigating Log4Shell and Other Log4j-Related Vulnerabilities," December 23, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a.

———. "The Urgent Need for Memory Safety in Software Products," September 20, 2023. https://www.cisa.gov/news-events/news/urgent-need-memory-safety-software-products.

Crosby, Kevin. "Securing the Supply Chain at Scale: Starting with 71 Important Open Source Projects." The GitHub Blog, August 11, 2025. https://github.blog/open-source/maintainers/securing-the-supply-chain-at-scale-starting-with-71-important-open-source-projects/.

Crouse, Megan. “Software Makers Encouraged to Stop Using C/C++ by 2026.” TechRepublic, November 4, 2024. https://www.techrepublic.com/article/cisa-fbi-memory-safety-recommendations/.

———. “What’s Next for Open Source Software Security in 2025?” TechRepublic, January 9, 2025. https://www.techrepublic.com/article/open-source-software-security-trends-2025/.

De Noni, Ivan, Andrea Ganzaroli, and Luigi Orsi. “The Evolution of OSS Governance: A Dimensional Comparative Analysis.” *Scandinavian Journal of Management* 29, no. 3 (September 2013): 247–63. https://doi.org/10.1016/j.scaman.2012.10.003.

DevHunt. “OSS Developer Best Practices.” Accessed March 30, 2025. https://devhunt.org/blog/oss-developer-best-practices.

Dierking, Niklas. “Linux Foundation and OpenSFF Help to Implement the Requirements of the CRA.” heise online, February 9, 2025. https://www.heise.de/en/news/Linux-Foundation-and-OpenSFF-help-to-implement-the-requirements-of-the-CRA-10275663.html.

European Commission. “Cyber Resilience Act | Shaping Europe’s Digital Future.” Accessed March 6, 2025. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

European Parliament. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), 2024/2847 § (2024). http://data.europa.eu/eli/reg/2024/2847/oj/eng.

“Executive Order No. 14028, Improving the Nation’s Cybersecurity.” Federal Register 86, no. 93 (May 17, 2021): 26633–26647. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

Finlay, Rebecca, and Mark Surman. “Innovation & Safety Are Products of Open Source.” Tech Policy Press, August 14, 2024. https://techpolicy.press/innovation-safety-are-products-of-open-source.

GeeksforGeeks. “What Is HTTP ?” GeeksforGeeks, April 1, 2024. https://www.geeksforgeeks.org/html/what-is-http/.

Geer, Dan, and Paul Rosenzweig. “Importance of Standards to National Security.” Lawfare, February 6, 2023. https://www.lawfaremedia.org/article/importance-of-standards-to-national-security.

“GitHub Security Features.” GitHub Docs. Accessed September 29, 2025. https://docs.github.com/en/code-security/getting-started/github-security-features.

Hafner, Katie, and Matthew Lyon. *Where Wizards Stay Up Late: The Origins of the Internet*. Simon & Schuster, Inc., 1996.

Harris, David Evan. “How to Regulate Unsecured ‘Open-Source’ AI: No Exemptions.” Tech Policy Press, December 4, 2023. https://techpolicy.press/how-to-regulate-unsecured-opensource-ai-no-exemptions.

Henning, Bree. “The Importance of the Open Security Standard (OSS) for Modern Access Control Systems.” Blue-id.com, June 2024. https://www.blue-id.com/en/blog/the-importance-of-open-security-standard-for-modern-access-control-systems.

Herman, Michele. “Sensible Open Source Licenses For Standards Development Organizations.” SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, October 22, 2020. https://doi.org/10.2139/ssrn.3717031.

Hoffmann, Manuel, Frank Nagle, and Yanuo Zhou. “The Value of Open Source Software.” *Harvard Business School,* 2024. https://doi.org/10.2139/ssrn.4693148.

IBM.com. “What Is a Zero-Day Exploit?,” June 2, 2023. https://www.ibm.com/think/topics/zero-day.

IBM.com. “What Is Log4Shell?,” August 15, 2023. https://www.ibm.com/think/topics/log4shell.

IETF HTTP Working Group. “IETF HTTP Working Group.” https://httpwg.org/.

ISO. "ISO 9001 - Quality Management Systems Requirements," 2015. https://www.iso.org/standard/62085.html.

Kinza, Yasar, Mary E. Shacklett, and Amy Novotny. "What Is TCP/IP and How Does It Work? | TechTarget." *TechTarget* (blog), September 2024. https://www.techtarget.com/searchnetworking/definition/TCP-IP.

Kirichenko, David. "Predictions for Open Source Security in 2025: AI, State Actors, and Supply Chains." OpenSSF, January 2025. https://openssf.org/blog/2025/01/23/predictions-for-open-source-security-in-2025-ai-state-actors-and-supply-chains/.

Laat, Paul B. de. "Governance of Open Source Software: State of the Art." *Journal of Management & Governance* 11, no. 2 (May 1, 2007): 165–77. https://doi.org/10.1007/s10997-007-9022-9.

Linskens, Aaron. "A Guide for Open Source Software (OSS) Security." *Sonatype* (blog), May 10, 2024. https://www.sonatype.com/blog/a-guide-for-open-source-software-oss-security.

Lohr, Steve. "An Industry Insider Drives an Open Alternative to Big Tech's A.I." *The New York Times*, October 19, 2023, sec. Technology. https://www.nytimes.com/2023/10/19/technology/allen-institute-open-source-ai.html.

Lord, Bob, and Jack Cable. "Leading the Way with Radical Transparency." CISA.gov, July 18, 2023. https://www.cisa.gov/news-events/news/leading-way-radical-transparency.

Nagle, Frank. "How to Prioritize the Improvement of Open-Source Software Security." Brookings, March 2, 2022. https://www.brookings.edu/articles/how-to-prioritize-the-improvement-of-open-source-software-security/.

National Fire Protection Association. "The Value of Standards Development Organizations." Accessed March 30, 2025. https://www.nfpa.org/for-professionals/codes-and-standards/standards-development/the-value-of-standards-development-organizations.

NIST. "Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028," July 7, 2021. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or.

Oladimeji, Saheed and Sean Michael Kerner. "Solarwinds Hack Explained: Everything You Need to Know." TechTarget, November 3, 2023. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

Open Source Initiative. "Open Standards Requirement for Software," July 24, 2006. https://opensource.org/osr.

Open Source Initiative. "What Is the Cyber Resilience Act and Why It's Dangerous for Open Source," January 24, 2023. https://opensource.org/blog/what-is-the-cyber-resilience-act-and-why-its-important-for-open-source.

OpenForum Europe and European Commission. "Standards and Open Source: Bringing Them Together," November 2017. https://openforumeurope.org/publications/standards-and-open-source-bringing-them-together/.

OpenSSF. "Understanding the CRA: OpenSSF's Role in the Cyber Resilience Act Implementation – Part 1 – Open Source Security Foundation," November 25, 2024. https://openssf.org/blog/2024/11/25/understanding-the-cra-openssfs-role-in-the-cyber-resilience-act-implementation-part-1/.

"Ossf/Wg-Best-Practices-Os-Developers." JavaScript. 2020. Reprint, github.com: Open Source Security Foundation (OpenSSF), April 4, 2025. https://github.com/ossf/wg-best-practices-os-developers.

Profitt, Brian. "Setting up Governance for an Open Source Project." RedHat, February 27, 2023. https://www.redhat.com/en/resources/setting-up-governance-whitepaper.

Rep. Green, Mark E. Securing Open Source Software Act of 2023, H.R.3286 § (2023). https://www.congress.gov/bill/118th-congress/house-bill/3286/all-info.

Rep. Michael McCaul. Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 118–278 (2018). https://www.congress.gov/bill/115th-congress/house-bill/3359?s=2&r=19.

Sen. Thomas R. Carper. Federal Information Security Modernization Act of 2014, Pub. L. No. 113–218 (2014). https://www.congress.gov/bill/113th-congress/senate-bill/2521.

Sharma, Chinmayi, John Speed Meyers, and James Howison. "The Securing Open Source Software Act Is Good, but Whatever Happened to Legal Liability?" Lawfare, November 10, 2022. https://www.lawfaremedia.org/article/securing-open-source-software-act-good-whatever-happened-legal-liability.

Shortridge, Kelly. "RE: Doc. No. ONCD-2023-0002; Request for Information on Open-Source Software Security: Areas of Long-Term Focus and Prioritization," November 2, 2023. https://kellyshortridge.com/papers/ONCD-2023-0002-Shortridge-Sensemaking.pdf.

"Software Security in Supply Chains: Open Source Software Controls." *NIST*, May 3, 2022. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-open.

"Software Security in Supply Chains: Software Bill of Materials (SBOM)." NIST, November 1, 2024. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1.

"Solarwinds Supply Chain Attack." Fortinet. Accessed September 29, 2025. https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack.

Spring, Jonathan M., and Phyllis Illari. "Review of Human Decision-Making during Computer Security Incident Analysis." *Digital Threats: Research and Practice* 2, no. 2 (June 30, 2021): 1–47. https://doi.org/10.1145/3427787.

Standards Coordinating Body. "Standards Development Process." Accessed March 8, 2025. https://www.standardscoordinatingbody.org/standards-process.

Technical Advisory Council. "Report to the CISA Director on Open Source Security." CISA Cybersecurity Advisory Committee, October 11, 2024. https://www.cisa.gov/sites/default/files/2024-10/CSAC_TAC_Recommendations-Open%20Source_20241011_508.pdf.

The Linux Foundation. "New Open Source Contributor Report from Linux Foundation and Harvard Identifies Motivations and Opportunities for Improving Software Security," December 8, 2020. https://www.linuxfoundation.org/press/new-open-source-contributor-report-from-linux-foundation-and-harvard-identifies-motivations-and-opportunities-for-improving-software-security.

———. "The Linux Foundation and Harvard's Lab for Innovation Science Release Census for Open Source Software Security," February 18, 2020. https://www.linuxfoundation.org/press/the-linux-foundation-and-harvards-lab-for-innovation-science-release-census-for-open-source-software-security.

The Solarwinds Cyberattack explained: Hack, victims, and key facts. September 21, 2025. https://www.futurescope.co/solarwinds-cyberattack/.

The White House. "FACT SHEET: Biden-Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan," July 13, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/.

———. "National Cybersecurity Strategy Implementation Plan," July 2023. https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

theopensourceway. "Project and Community Governance." GitHub. Accessed November 25, 2024. https://github.com/theopensourceway/guidebook/blob/main/community_governance.adoc.

unicode.org. "FAQ - Standards Developing Organizations." Accessed March 30, 2025. https://www.unicode.org/faq/sdos.html.

Ward, David. "Three Years On: Open Standards, Open Source, Open Loop." *Cisco Blogs* (blog), February 6, 2018. https://blogs.cisco.com/sp/three-years-on-open-standards-open-source-open-loop.

Weiser, Philip J. "Internet Governance, Standard Setting, and Self-Regulation." *Northern Kentucky Law Review* 28:4 (2001).

Whiting, Dan. “Why Do Enterprises Use and Contribute to Open Source Software.” The Linux Foundation, June 2, 2022. https://www.linuxfoundation.org/blog/blog/why-do-enterprises-use-and-contribute-to-open-source-software.

Wright, Nataliya L., Frank Nagle, and Shane Greenstein. “Breaking Down Walls: How Open Source Software Drives Entrepreneurial Activity.” Columbia Business School, April 30, 2024. https://business.columbia.edu/research-brief/research-brief/breaking-down-walls-how-open-source-software-entrepreneurship.

Endnotes

1 "The Linux Foundation and Harvard's Lab for Innovation Science Release Census for Open Source Software Security," The Linux Foundation, February 18, 2020, https://www.linuxfoundation.org/press/the-linux-foundation-and-harvards-lab-for-innovation-science-release-census-for-open-source-software-security.

2 Llama is Meta's flagship large-language mode (LLM). It is not completely open-sourced, since the full details of its training and construction are not publicly available, but its model weights are public, and it is freely downloadable with adjustable weights. Log4Shell is a widespread critical vulnerability in an OSS program, and it is described in deeper detail later in this paper. The SolarWinds breach is a commercial software incident found in 2020.

3 Danny Bradbury, "When Software Depends on a Project Thanklessly Maintained by a Random Guy in Nebraska, Is Open Source Sustainable?," May 10, 2021, https://www.theregister.com/2021/05/10/untangling_open_sources_sustainability_problem/.

4 "New Open Source Contributor Report from Linux Foundation and Harvard Identifies Motivations and Opportunities for Improving Software Security," The Linux Foundation, December 8, 2020, https://www.linuxfoundation.org/press/new-open-source-contributor-report-from-linux-foundation-and-harvard-identifies-motivations-and-opportunities-for-improving-software-security.

5 Interview with American OSS Foundation Staffer - 2/19/25

6 DevHunt. "OSS Developer Best Practices." Accessed March 30, 2025. https://devhunt.org/blog/oss-developer-best-practices.

7 Rudi Bekkers and Dongback Seo, "Importance and Comparison of Standard Development Organizations in the Ubiquitous Society," January 2008, https://www.researchgate.net/publication/255579802_Importance_and_comparison_of_standard_development_organizations_in_the_ubiquitous_society.

8 Ibid.

9 Standards Coordinating Body. "Standards Development Process." Accessed March 8, 2025. https://www.standardscoordinatingbody.org/standards-process.

10 "FAQ - Standards Developing Organizations," unicode.org, accessed March 30, 2025, https://www.unicode.org/faq/sdos.html.

11 "What Is ANSI?," ANSI, accessed March 30, 2025, https://share.ansi.org/Shared%20Documents/News%20and%20Publications/Brochures/WhatIsANSI_brochure.pdf.

12 "Open Standards Requirement for Software," Open Source Initiative, July 24, 2006, https://opensource.org/osr.

13 Yasar Kinza, Mary E. Shacklett, and Amy Novotny, "What Is TCP/IP and How Does It Work? | TechTarget," TechTarget (blog), September 2024, https://www.techtarget.com/searchnetworking/definition/TCP-IP.

[14] GeeksforGeeks. "What Is HTTP ?" GeeksforGeeks, April 1, 2024. https://www.geeksforgeeks.org/html/what-is-http/.

[15] IETF HTTP Working Group. "IETF HTTP Working Group." https://httpwg.org/.

[16] "What Is Log4Shell?," IBM.com, August 15, 2023, https://www.ibm.com/think/topics/log4shell.

[17] "Mitigating Log4Shell and Other Log4j-Related Vulnerabilities," CISA.gov, December 23, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a.

[18] "What Is a Zero-Day Exploit?," IBM.com, June 2, 2023, https://www.ibm.com/think/topics/zero-day.

[19] "What Is Log4Shell?," IBM.com.

[20] Ibid.

[21] Ibid.

[22] "2022 Top Routinely Exploited Vulnerabilities," CISA.gov, August 3, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a.

[23] Interview with Former U.S. Federal Government Official - 2/26/25

[24] Interview with American Cybersecurity Professional - 2/12/25

[25] The Solarwinds Cyberattack explained: Hack, victims, and key facts. September 21, 2025. https://www.futurescope.co/solarwinds-cyberattack/.

[26] "Solarwinds Supply Chain Attack," Fortinet, accessed September 29, 2025, https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack.

[27] Saheed Oladimeji and Sean Michael Kerner, "Solarwinds Hack Explained: Everything You Need to Know," TechTarget, November 3, 2023, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

[28] Rajeev Bera, "Strengthening Open Source Software: Best Practices for Enhanced Security – Open Source Security Foundation," OpenSSF, n.d., https://openssf.org/blog/2023/09/06/strengthening-open-source-software-best-practices-for-enhanced-security/.

[29] Mark E. Rep. Green, "Securing Open Source Software Act of 2023," H.R.3286 § (2023), https://www.congress.gov/bill/118th-congress/house-bill/3286/all-info.

[30] Interview with American Congressional Staffer, 2/7/25

[31] CISA, "CISA Open Source Software Security Roadmap," September 12, 2023, https://www.cisa.gov/resources-tools/resources/cisa-open-source-software-security-roadmap.

[32] Ibid.

[33] "Executive Order No. 14028, Improving the Nation's Cybersecurity." Federal Register 86, no. 93 (May 17, 2021): 26633–26647. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[34] "Software Security in Supply Chains: Software Bill of Materials (SBOM)," NIST, November 1, 2024, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1.

[35] Ivan De Noni, Andrea Ganzaroli, and Luigi Orsi, "The Evolution of OSS Governance: A Dimensional Comparative Analysis," Scandinavian Journal of Management 29, no. 3 (September 2013): 247–63, https://doi.org/10.1016/j.scaman.2012.10.003.

[36] Chakraborti, Mahasweta, Curtis Atkisson, Ştefan Stănciulescu, Vladimir Filkov, and Seth Frey. "Do We Run How We Say We Run? Formalization and Practice of Governance in OSS Communities." In Proceedings of the 2024 CHI Conference

on Human Factors in Computing Systems, 1–26. CHI '24. New York, NY, USA: Association for Computing Machinery, 2024. https://doi.org/10.1145/3613904.3641980.

37 Brian Profitt, "Setting up Governance for an Open Source Project" (RedHat, February 27, 2023), https://www.redhat.com/en/resources/setting-up-governance-whitepaper.

38 David Kirichenko, "Predictions for Open Source Security in 2025: AI, State Actors, and Supply Chains," OpenSSF, January 2025, https://openssf.org/blog/2025/01/23/predictions-for-open-source-security-in-2025-ai-state-actors-and-supply-chains/.

39 Crouse, Megan. "What's Next for Open Source Software Security in 2025?" TechRepublic, January 9, 2025. https://www.techrepublic.com/article/open-source-software-security-trends-2025/.

40 OpenForum Europe and European Commission. "Standards and Open Source: Bringing Them Together," November 2017. https://openforumeurope.org/publications/standards-and-open-source-bringing-them-together/.

41 Herman, Michele. "Sensible Open-Source Licenses For Standards Development Organizations." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, October 22, 2020. https://doi.org/10.2139/ssrn.3717031.

42 Ibid.

43 "Ossf/Wg-Best-Practices-Os-Developers," JavaScript (2020; repr., github.com: Open Source Security Foundation (OpenSSF), April 4, 2025), https://github.com/ossf/wg-best-practices-os-developers.

44 Linskens, Aaron. "A Guide for Open Source Software (OSS) Security." Sonatype (blog), May 10, 2024. https://www.sonatype.com/blog/a-guide-for-open-source-software-oss-security.

45 Henning, Bree. "The Importance of the Open Security Standard (OSS) for Modern Access Control Systems." Blue-id.com, June 2024. https://www.blue-id.com/en/blog/the-importance-of-open-security-standard-for-modern-access-control-systems.

46 Dan Whiting, "Why Do Enterprises Use and Contribute to Open Source Software," The Linux Foundation, June 2, 2022, https://www.linuxfoundation.org/blog/blog/why-do-enterprises-use-and-contribute-to-open-source-software.

47 Interview with American OSS Community Leader - 2/12/25

48 Interview with American University Professor - 2/11/25

49 As described in: Katie Hafner and Matthew Lyon, Where Wizards Stay up Late: The Origins of the Internet (Simon & Schuster, Inc., 1996).

50 Interview with European OSS Community Leader, 2/25/25

51 Luckily, this scenario presently seems unlikely given the allowances made for OSS in recent software legislation like the EU AI Act and Cyber Resilience Act.

52 Standards Coordinating Body. "Standards Development Process."

53 National Fire Protection Association, "The Value of Standards Development Organizations," accessed March 30, 2025, https://www.nfpa.org/for-professionals/codes-and-standards/standards-development/the-value-of-standards-development-organizations.

54 Interview with American OSS Foundation Staffer – 2/19/25

55 Ibid.

56 Interview with European OSS Community Leader - 2/25/25

57 European Parliament, "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No

168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)," 2024/2847 § (2024), http://data.europa.eu/eli/reg/2024/2847/oj/eng.

58 Kevin Crosby, "Securing the Supply Chain at Scale: Starting with 71 Important Open Source Projects," The GitHub Blog, August 11, 2025, https://github.blog/open-source/maintainers/securing-the-supply-chain-at-scale-starting-with-71-important-open-source-projects/.

59 CISA.gov, "The Urgent Need for Memory Safety in Software Products," September 20, 2023, https://www.cisa.gov/news-events/news/urgent-need-memory-safety-software-products.

60 Megan Crouse, "Software Makers Encouraged to Stop Using C/C++ by 2026," TechRepublic, November 4, 2024, https://www.techrepublic.com/article/cisa-fbi-memory-safety-recommendations/.

61 Open Source Security Foundation, "Best Practices Badge," accessed April 3, 2025, https://openssf.org/best-practices-badge/.

62 Interview with American University Researcher – 2/6/25

63 CISA.gov, "CISA Announces New Efforts to Help Secure Open Source Ecosystem," March 7, 2024, https://www.cisa.gov/news-events/news/cisa-announces-new-efforts-help-secure-open-source-ecosystem.

64 Anonymous Interview with American University Professor, 2/11/25

65 "GitHub Security Features," GitHub Docs, accessed September 29, 2025, https://docs.github.com/en/code-security/getting-started/github-security-features.

66 Hoffmann, Manuel, Frank Nagle, and Yanuo Zhou. "The Value of Open Source Software." Harvard Business School, 2024. https://doi.org/10.2139/ssrn.4693148.

The Stimson Center promotes international security and shared prosperity through applied research and independent analysis, global engagement, and policy innovation.

STIMSON.ORG

STIMSON

INNOVATIVE IDEAS CHANGING THE WORLD