May 2023 · Dr. Sven Herpig

# Fostering Open Source Software Security

## Blueprint for a Government Cybersecurity Open Source Program Office

Stiftung
Neue
Verantwortung

Think Tank at the Intersection of Technology and Society

## Acknowledgment

This analysis was supported by the Transatlantic Cyber Forum working group on the "Government's Role In Increasing IT Security of Open-Source Software" (GRITOSS) through a pre-workshop, researcher and practitioner interviews, online collaboration and a joint workshop in Berlin. The views and opinions expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the working group members or that of their respective employer(s). In alphabetical order, the author acknowledges the essential contributions of the following individuals:

1. Charles-Pierre Astolfi, Élément déclencheur SAS
2. Lola Attenberger, Carl Zeiss SMT GmbH
3. Manuel Atug, AG KRITIS
4. William Bartholomew, Microsoft
5. Zoë Brammer, Institute for Security and Technology
6. Gregor Bransky, Innovationsverbund Öffentliche Gesundheit e.V.
7. Jack Cable, Cybersecurity and Infrastructure Security Agency
8. Isabel Drost-Fromm, Europace AG
9. Lars Fischer, Bremerhaven University of Applied Science
10. Kenneth Geers, Atlantic Council
11. Maia Hamin, Atlantic Council
12. Trey Herr, Atlantic Council
13. Danilo Kampe, D-TRUST GmbH
14. Fiona Krakenbürger, Sovereign Tech Fund
15. Caroline Krohn, AG Nachhaltige Digitalisierung
16. Andreas Kuehn, Observer Research Foundation America
17. Thomas Lawson, AXA
18. Eugenia Lostri, Lawfare Institute
19. Jamie MacColl, Royal United Services Institute
20. Astor Nummelin Carlberg, OpenForum Europe
21. Alexandra Paulus, Stiftung Neue Verantwortung e.V.
22. Christine Runnegar, Internet Society
23. Alexander Sander, Free Software Foundation Europe
24. Stewart Scott, Atlantic Council
25. Miriam Seyffarth, Open Source Business Alliance - Bundesverband für digitale Souveränität e.V.
26. Frank Termer, Bitkom e.V.

Additionally, the author would like to thank the contributors who participated in the open consultation process, including Thomas Caspers.

Furthermore, the author would like to extend the utmost thanks to the Atlantic Council's Cyber Statecraft Initiative and the Open Source Policy Network, without which this project would not have come to life.

Finally, the author would like to thank Frederic Dutke, Christina Rupp and Julia Schuetze for their support in designing and implementing the workshop, as well as Luisa Seeling, Alina Siebert and Scribendi Editor EM123 for their support with this publication.

# Executive Summary

Open source software (OSS) is the backbone and driver of digitization across sectors worldwide. This makes OSS a cornerstone of every society and economy, including the core of national security concerns. Therefore, governments have a vested interest in OSS security. At the same time, governments, as large users of OSS, bear some of the responsibility for supporting the OSS ecosystem.

To assume responsibility, governments must understand the existing OSS communities and the culture surrounding OSS. Governments will be able to effectively foster OSS security only if they work with the ecosystem stakeholders. Doing so requires governments to adhere to guidelines such as respect, cooperation, collaboration and sincerity. In addition, governments must identify their own role(s) in consultation with the OSS ecosystem. Governments can serve as internal coordinators, role models, supporters and regulators. The role of internal coordinator requires governments to be more transparent and systematic in their own use of OSS. In particular, they should take stock of what is being used, where exactly the components are being used and how they are used. As role models, governments engage with OSS, adhering to best practices in the ecosystem and encouraging other governments and stakeholders to do so. As supporters, governments actively engage with the OSS ecosystem, mobilizing and channeling resources into it through various means. Governments use their regulatory powers to create a legal framework that reflects the characteristics of the OSS ecosystem. They can mix and match from different roles and shift between them as they gain more experience, trust and credibility in the OSS ecosystem.

Taken together, these roles and guidelines provide an ideational framework for government action in the OSS ecosystem. However, to operationalize this framework, a government actor that is equipped with the necessary authority, resources and expertise must be identified or created. This task should ideally be taken over by an Open Source Program Office (OSPO). Mobilizing resources such as funds, capabilities and credibility, a *Cybersecurity OSPO*—either standalone or as part of a larger OSPO—can implement, coordinate and facilitate policy interventions for the shared goal of improving OSS security across the ecosystem.

**It is important that governments understand their responsibility and allocate resources for a more secure OSS ecosystem in a community-sensitive, structured and sustainable manner. This paper offers a blueprint for how governments can do this and where to start.**

# Table of Contents

# 1. Introduction

Open source software (OSS)[1] is one of the most important elements of digital infrastructure worldwide. Studies show that between 78% and 96% of any software stack consists of OSS[2]. Additionally, "more than half the critical infrastructure codebases analyzed depends on open source"[3]. Or simply put, "[open source] is now being used by everyone, everywhere"[4]. The importance of OSS is unlikely to decline, as its economic value and potential—as they are understood thus far—are immense.[5] In 2021, a European Union (EU) study concluded that "it is estimated that companies located in the EU invested around €1 billion in OSS in 2018, which resulted in an impact on the European economy of between €65 and €95 billion"[6]. Although such studies, and thus concretely quantified empirical bases, are rare[7], they provide a good estimate.

The dependence of economies and societies on OSS means that its security is of pivotal importance for governments and national security.[8] The exploitation of OSS vulnerabilities can have a far-reaching impact, a lesson that vulnerabilities such as Heartbleed[9], discovered in 2014, and more recently, Log4Shell[10] have highlighted. Therefore, securing OSS should be high on the policy agenda for every government that takes cybersecurity seriously. However, "government interventions have been lacking," and without them, "open-source resources will be depleted, rendering our most important systems vulnerable to attack"[11]. Apart from isolated initiatives, such as limited bug bounties (including EU-FOSSA/-FOSSA 2)[12], selected code audits (including Truecrypt)[13] and guides (including the Recommended Practices Guide for Developers)[14],

[1] For the OSS definition used in this paper, see open source initiative (2007): The Open Source Definition

[2] Sonatype (2021): 2020 State of the Software Supply Chain and the Black Duck Audit of 1,703 codebases for the Synopsys (2023): Open Source Security And Risk Analysis Report

[3] Chinmayi Sharma (2022): Tragedy of the Digital Commons based on the Black Duck Audit of 2,409 commercial codebases for the Synopsys (2022): 2022 Open Source Security And Risk Analysis Report

[4] Chinmayi Sharma (2022): Tragedy of the Digital Commons

[5] Frank Nagle (2022): Strengthening digital infrastructure: A policy agenda for free and open source software and European Commission, Fraunhofer ISI and OpenForum Europe (2021): The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy

[6] European Commission, Fraunhofer ISI and OpenForum Europe (2021): The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy

[7] OECD iLibrary (2019): 5.7. Roadmap: Measuring open source software and swissICT (2015): Open Source Studie Schweiz 2015

[8] Varun Badhwar (2022): The Government's Role in Maintaining Open-Source Security

[9] See, for example, Cybersecurity & Infrastructure Security Agency (2018): OpenSSL Vulnerability

[10] See, for example, Bundesamt für Sicherheit in der Informationstechnik (2022): Kritische „Log4Shell" Schwachstelle in weit verbreiteter Protokollierungsbibliothek Log4j (CVE-2021-44228) and Dialog für Cybersicherheit (2023): Log4shell & Consequences

[11] Chinmayi Sharma (2022): Tragedy of the Digital Commons

[12] Ionut Ilascu (2018): The EU Opens Bug Hunting Season in 2019 for 15 Open-Source Projects It Uses and European Commission Directorate-General for Informatics (2021): European Commission launches new Open Source Bug Bounties and European Commission (2022): EU-FOSSA 2 - Free and Open Source Software Auditing

[13] Bundesamt für Sicherheit in der Informationstechnik (2015): Sicherheitsanalyse TrueCrypt

[14] Office of the Director of National Intelligence et al (2022): Securing the Software Supply Chain – Recommended Practices Guide For Developers

governments and supra-national bodies have not prioritized engaging coherently in securing OSS until recently.[15]

In 2022, driven by the effects of Log4Shell and other security events, “open source attracted unprecedented attention from governments and the global policy community”[16]. Countries such as the United States and Germany have moved securing OSS up their priority lists. In the United States, the topic landed on the agenda of the White House, which hosted its first Open Source Security Summit in January 2022[17] followed by congressional hearings[18] and the introduction of the Securing Open Source Software Act of 2022 in the U.S. Senate[19]. Germany responded to OSS-related security incidents by adding more stakeholders to its vast cybersecurity architecture.[20] It created the Sovereign Tech Fund (STF)[21] in October 2022 and the Center for Digital Sovereignty (ZenDIS)[22] in December 2022. Both institutions aim to improve the OSS ecosystem[23], including, but not limited to, its security.

Experts agree that governments can play a role in improving the security of the OSS ecosystem[24]. However, it does not appear as if they have properly identified their potential roles in this ecosystem and subsequently linked them to a coherent set of coordinated policy interventions. Engaging with the complex OSS ecosystem consisting of commercial entities as well as communities, volunteers and foundations[25] is not an easy task for governments. This was highlighted in 2022 by the criticism regarding the OSS provisions in the proposed EU Cyber Resilience Act (CRA), which seems to overburden OSS maintainers and contributors rather than improve product security.[26]

[15] A database for government OSS policies can be found at Center For Strategic & International Studies (2023): Government Open Source Software Policies
[16] Mike Linksvayer (2022): The changing nature of governmental policies around open source
[17] The White House (2022): Readout of White House Meeting on Software Security
[18] U.S. Congress (2022): Securing the Digital Commons: Open-Source Software Cybersecurity and U.S. Senate Committee on Homeland Security & Governmental Affairs (2022): Responding To And Learning From The Log4Shell Vulnerability
[19] U.S. Congress (2022): Securing Open Source Software Act of 2022
[20] Stiftung Neue Verantwortung (2023): Germany’s Cybersecurity Architecture
[21] Sovereign Tech Fund (2023): Stärkung von digitalen Infrastrukturen und Open-Source-Ökosystemen im öffentlichen Interesse
[22] Der Beauftragte der Bundesregierung für Informationstechnik (2022): Zentrum für Digitale Souveränität der öffentlichen Verwaltung
[23] An introduction to the OSS ecosystem(s) can be found in Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure
[24] See, for example, U.S. Congress (2022): Securing the Digital Commons: Open-Source Software Cybersecurity
[25] Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure
[26] See, for example, Maarten Aertsen (2022): Open-source software vs. the proposed Cyber Resilience Act and Aeva Black and Gil Yehuda (2022): Open Source Security Policy Conundrum and Olaf Kolkman (2022): The EU’s Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem

Although much has been written about improving the OSS ecosystem in terms of security, one aspect that has not received much attention is the government's role and structure.[27] The first step in streamlining and coordinating government OSS policy interventions may be to set up one or more government Open Source Program Offices (OSPOs)[28]. OSPOs should generally—within and outside governments—be "designed to be the center of competency for an organization's open source operations and structure"[29].

However, dealing with cybersecurity aspects adds a layer of challenges and a set of unique characteristics to the mix. As cybersecurity is one of the political demands that drive the creation of OSPOs[30], governments may want to prioritize this topic when setting up their OSPOs. A government OSPO with a dedicated cybersecurity focus may not need to be a self-contained OSPO. It can also be part of a larger government OSPO that is formally and/or informally connected to other parts. For ease of use, therefore, the Government Cybersecurity Open Source Program Office discussed in this paper will be referred to—independent of its ultimate institutional setup—as *Cybersecurity OSPO*.

**Of course, empirical data on the viability of a specialized institution like a Cybersecurity OSPO is lacking. This explorative paper is meant to be the first in a series of iterations. Further research is necessary, including empirical testing and validation, to delve deeper into this topic[31]. Valuable feedback from researchers and other stakeholders regarding the presented model is greatly appreciated.**

The relationship between government OSPOs and a Cybersecurity OSPO may be likened to the relationship between the Chief Information Officer (CIO) or Chief Technology Officer (CTO) and Chief Information Security Officer (CISO). The CIO and CTO focus on managing information technology and the corresponding resources, and the CISO ensures that digitization takes place as securely as possible. In this constellation, the CISO is ideally as independent from the CIO/CTO as possible[32] while working toward the shared goal of an effective and secure digital infrastructure.

[27] Aligning with the finding that "[o]ver the past few years, there have been many government and industry efforts to improve security practices in open source, although most of them have been more focused on what needs to be done than who is going to do the work" in Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report.

[28] Chris Aniszczyk, Jeff McAffer, Will Norris and Andrew Spyker (2023): Creating an Open Source Program and Chris Aniszczyk, Gil Yehuda and Tulio Leao (2022): Open Source Program Office (OSPO) Definition and Guide and Brian Proffitt (2019): What does an open source program office do? and Ibrahim Haddad (2022): A Deep Dive Into Open Source Program Offices - Structure, Roles, Responsibilities, and Challenges

[29] Chris Aniszczyk, Gil Yehuda and Tulio Leao (2022): Open Source Program Office (OSPO) Definition and Guide

[30] OpenForum Europe and The OSPO Alliance (2022): The OSPO - A New Tool for Digital Government

[31] Trey Herr, Robert Morgus, Stewart Scott and Tianjiu Zuo (2022): Buying down risk: Open source software

[32] Bundesamt für Sicherheit in der Informationstechnik (2017): BSI-Standard 200-2 and ISACA Germany Chapter (2016): Implementierungsleitfaden ISO/IEC 27001:2013

After an overview of OSS security, this paper discusses the guidelines that may enable government action and the roles governments could assume in the OSS ecosystem. Building on this, the paper presents a Cybersecurity OSPO blueprint that includes its possible location in the existing government stakeholder architecture, a list of relevant policy interventions and required resources. The blueprint is followed by an outline of the first steps that may help bring the Cybersecurity OSPO to life.

**Equipped with this blueprint, governments will hopefully be better able to assume their shared responsibility[33] for a more secure OSS ecosystem.**

[33] Zoë Brammer, Silas Cutler, Marc Rogers and Megan Stifel (2023): Castles Built On Sand - Towards Securing The Open-Source Software Ecosystem

## 2. Open Source Software Security

Software is considered open source if its license meets the criteria of the Open Source Definition (OSD)[34] and has been verified by the Open Source Initiative (OSI)[35]. The OSD criteria pertain to redistribution, source code, derived works, integrity of the author's source code, discrimination against persons, groups or fields of endeavor, distribution of license, product specificity, software restrictions and technology-neutrality.[36] Often, it is simply stated that "[o]pen source software is code that is designed to be publicly accessible—anyone can see, modify, and distribute the code as they see fit"[37]. This public access is a key feature of OSS security, as it enables independent code reviews and third-party patches in addition to its use and redistribution by all.

The OSS ecosystem is extremely heterogeneous, covering everything from individuals who develop and maintain software in their spare time[38] to the OSS foundation[39] and multinational companies, such as Google, Red Hat and Microsoft,[40] across sectors such as fintech[41] and energy transition[42]. The composition of this ecosystem combined with the wide range of usage may be the main reason why it is difficult to describe the current state of OSS security. However, surveys and analyses conducted on the topic of OSS security allow for an approximation.[43] The reports examine various aspects, such as existing vulnerabilities and their patch provision, complexity of tracking dependencies and their state of security, as well as the level of maintenance and number of maintainers of OSS projects.[44] The security of any given OSS component depends on many factors, such as the programming language used, maintenance of direct and transitive dependencies[45], the size of the developer team, the levels of independent code reviews and the criticality and exploitability of existing vulnerabilities.

[34] open source initiative (2007): The Open Source Definition.
[35] open source initiative (2007): OSI Approved Licenses
[36] open source initiative (2007): The Open Source Definition
[37] Red Hat (2019): What is open source?
[38] Ruth Fulterer (2021): Log4j wurde 1997 in der Schweiz entwickelt – der Erfinder erzählt and Dialog für Cybersicherheit (2023): Log4shell & Consequences and xkcd (2023): Dependency and Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report
[39] For example The Linux Foundation, Open Source Security Foundation or the Eclipse Foundation.
[40] Osci (2023): Open Source Contributor Index and Felipe Hoffa (2018): Who contributed the most to open source in 2017 and 2018? Let's analyze GitHub's data and find out
[41] FINOS (2023): Fintech Open Source Foundation
[42] LF Energy (2023): Leading the energy transition through global open source collaboration
[43] See Annex A.
[44] See Annex A.
[45] "Dependencies are a characteristic of modern development. Direct dependencies are typically components or services called directly by your code. Indirect or transitive dependencies are essentially dependencies of your dependencies (in typically many tiers)", Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software

It is, however, difficult to judge the state of software security in absolute terms. Although metrics such as "29% of the 10% most popular OSS projects contained at least one known security vulnerability"[46] may seem high, and metrics such as "40% of the most used OSS packages had equal to or fewer than 5 maintainers"[47] may seem low, there is no shared understanding of what constitutes a good security level. The goal therefore should be to improve security metrics over time. In this respect, it is helpful that open source software is inherently transparent, which makes it easier to track and assess progress in security.

Widespread use, integration in products without proper security checks and lack of transparency of the components used across the software supply chain[48] are major factors that contribute to the existing OSS threat landscape. It is certainly safe to assume that the current state of OSS security, the attack surface, and the complex ecosystem and the importance of OSS for society and economy taken together warrant interventions by various stakeholders.[49]

Across stakeholder groups, such as non-government organizations and OSS communities, there are a multitude of recommendations for what to do at various levels[50], as well as initiatives and instruments[51]. One of the most recent pushes is the Open Source Security Foundation's (OpenSSF) Open Source Software Security Mobilization Plan.[52] Governments already play an active role in several initiatives. The U.S. government, for example, promotes instruments such as the Software Bill of Materials (SBOM)[53] and served as the convenor for what became the mobilization plan. The German government took a more institutionalized approach with the setup of the STF. In addition, of course, governments are often the stakeholders that provide funding or draft legislation. However, these interventions seem scattered and isolated, rather than following a coherent strategy for promoting OSS security. This should change.

[46] See Annex A for more details.

[47] See Annex A for more details.

[48] Alexandra Paulus and Christina Rupp (2023): Government's Role in Increasing Software Supply Chain Security

[49] This conclusion is by no means testimony to an inherent insecurity of OSS vis-à-vis closed software. Governments should encourage better security in closed software as well, to improve the overall state of cybersecurity. Additionally, most closed software includes OSS components, see Open Source Business Alliance (2022): Sicherheit: Open Source Software und proprietäre Software im Vergleich

[50] For example, Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure and Erin Farr (2022): 12 ways to improve your open source security and Trey Herr, Robert Morgus, Stewart Scott and Tianjiu Zuo (2022): Buying down risk: Open source software

[51] Open Source Security Foundation (2022): 2022 Annual Report and Michael Hill (2022): 8 notable open-source security initiatives of 2022 and sonatype (2020): 2020 State of the Software Supply Chain

[52] Open Source Security Foundation (2022): The Linux Foundation and Open Source Software Security Foundation (OpenSSF) Gather Industry and Government Leaders for Open Source Software Security Summit II and The Linux Foundation and Open Source Security Foundation (2022): The Open Source Software Security Mobilization Plan

[53] Cybersecurity And Infrastructure Security Agency (2023): Software Bill of Materials (SBOM)

# 3. Governments and Open Source Software Security

## 3.1 Guidelines for Government Actions

Demands that governments play an active role in improving OSS security[54], even if only as a source of funding, are ubiquitous in the OSS security policy ecosystem. However, details about the exact nature of this role are still mostly missing from the debate. If governments are to work successfully with other stakeholders in OSS security in the long term, it is vital for governments to clearly define their role in the process. As argued elsewhere, it should be "government support, tailored to both community needs and government priorities such as security or innovation, [that] can provide robust, stable backing for the existing patchwork of organizations and projects in the OSS world"[55].

However, governments need to take a community-sensitive approach when engaging with the OSS ecosystem. This is because "[o]pen source cannot be secured [solely] by the government or owners and operators of critical infrastructure assets that use open source; open-source security must involve the open-source community"[56]. Such an approach can be based on guidelines such as *respect*, *cooperation*, *collaboration* and *sincerity*.

**It is important to bear in mind that forming a working relationship is not a one-way street. Although governments can and should follow certain guidelines to effectively engage with stakeholders in the OSS ecosystem, some aspects of government behavior are unlikely to change. When approaching OSS communities, governments must clearly communicate where they are able and willing to compromise and where they are not. Both sides must engage in a process characterized by mutual respect. Ideally, this approach leads to an amalgam of best practices from both sides.**

### Respect

A coherent government approach to OSS security, including agencies and other state-backed stakeholders, requires a solid foundation. A helpful starting point is to review the values that characterize the OSS ecosystem: decentralization, openness and collaboration, among others. The OSS ecosystem is predicated on openness: Code is freely posted for anyone—at least to its users—to discuss and review. Projects and communities are governed by their main contributors within decentralized

[54] Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure
[55] Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure
[56] Chinmayi Sharma (2022): Tragedy of the Digital Commons

and heterogeneous structures. Governments should consider these values; ideally, any government initiative should reflect them. For example, that could mean that governments should avoid having only one centralized government-exclusive code repository and instead, contribute to existing ones used in the communities or open theirs up to other communities and allow for easy migration of projects. In terms of openness, governments may want to be very proactive in all communication efforts surrounding their OSS security actions and avoid setting up exclusive, closed OSS platforms[57]. One way to measure collaborativeness is through reciprocity. This means that, for example, if a stakeholder in the OSS ecosystem provides information about a security-related issue to the government, the government should at least acknowledge and respond to what has been done with that information. Furthermore, it is vital for governments to understand and embrace the community standards[58], collaboration style and diversity of OSS communities[59], as this allows for more meaningful and constructive engagement and cooperation.

### Cooperation

The government, OSS communities and other actors in the space have a shared interest in making OSS more secure. However, issues such as severe vulnerabilities in OSS used in critical infrastructures will inevitably lead to a debate regarding liability, especially at the political level. However, nothing will be achieved if governments try to regulate even the smallest OSS project. Shifting liability toward individual developers and maintainers may prompt them to limit accessibility to their projects or even end or abandon their projects altogether. Apart from the lack of resources that developers face, there is simply no incentive for them to comply with heavy-handed regulation. Developers often have no or limited resources. Poorly crafted regulations that impose significant costs (in money or time) on those unable to pay them are likely to result in developers not developing the software and/or not distributing the software in those regions, leading to poorer security. Therefore, governments must establish a very clear picture of the distribution of responsibility before engaging in OSS security.

The United States has recognized this in their new National Cybersecurity Strategy, which states: “Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users [...] nor on the open-source developer of a component that is integrated into a commercial product”[60]. That is not to say that there is no room for regulation. The debate surrounding the

[57] Lilith Wittmann (2021): Stellungnahme zur “Open Source-Plattform der Öffentlichen Verwaltung”

[58] Pointers from which community standards can be derived vary across communities. As an example, see The Apache Software Foundation Blog (2019): The Apache Way to Sustainable Open Source Success

[59] See, for example, The Mozilla Foundation and Open Tech Strategies (2018): Open Source Archetypes: A framework For Purposeful Open Source

[60] The White House (2023): National Cybersecurity Strategy

commercial provision in the CRA[61] will hopefully promote governments and OSS communities coming to stronger consensus on workable security regulation models for open source. Until then, it is in the best self-interest of governments to support individuals or smaller teams of developers and contributors—including micro, small and medium enterprises (MSMEs)—in this area. That support can come in many different forms, from funding and tax incentives to educational resources and even concrete tooling and guidelines.

### Collaboration

At the operational level, government staff works with developers, maintainers and contributors; people work with people. This requires trust, which is built in part through collaborating and becoming an active and responsible part of the communities. Certainly, people working in the government, for example, in national cybersecurity agencies, have been working and building trust with people in OSS communities. However, it is advisable for governments to assume that trust-building has to start from scratch, especially as individual relationships differ from institutional relationships. One way to start is to identify barriers that have stopped or complicated cooperation between government employees and OSS developers or contributors in the past. For example, it would be helpful to allow, and even incentivize, government employees to contribute to relevant OSS projects during their work time. Likewise, trust could be increased by enabling better information sharing by the employees back to the OSS ecosystem (reciprocity)—for example, regarding discovered vulnerabilities or detected security incidents, as well as in the form of product-specific security guidance.

### Sincerity

A surefire way to alienate OSS communities is to leverage the topic solely for political gain. As engaging in OSS security becomes more popular among governments, there is an increasing risk that they may attempt to fix a security problem by simply throwing money at it for a one-time solution, which often does not exist. This includes closed open-source platforms[62], organizing hackathons without follow-up measures or setting up isolated bug bounties without patch reward programs[63]. Governments need to take OSS and, consequently, OSS security seriously and make it a long-term commitment. Otherwise, governments risk losing the opportunity to work with OSS communities and other stakeholders to improve OSS security.

[61] See, for example, Maarten Aertsen (2022): Open-source software vs. the proposed Cyber Resilience Act and Aeva Black and Gil Yehuda (2022): Open Source Security Policy Conundrum and Olaf Kolkman (2022): The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem

[62] Lilith Wittmann (2021): Stellungnahme zur "Open Source-Plattform der Öffentlichen Verwaltung"

[63] Google Bug Hunters (2023): Patch Rewards Program Rules

Additionally, to show their sincerity, governments should review and adapt existing policies that spark distrust between OSS communities and governments. For example, policies such as computer crime laws regarding white hat hacking[64] or the potential use of reported vulnerabilities for intrusive cyber operations[65] need to be revised.

## 3.2 Different Roles Governments Can Assume

### 3.2.1 Government as an Internal Coordinator

*To fulfill this role, governments should follow primarily the guidelines of respect and collaboration.*

If governments decide to take on a more active and coherent role in fostering OSS security, reviewing their own structures might be a good starting point. It is vital that each part of the government understands which part serves as a coordinator and point of contact for OSS security. In this way, every government agency and all government institutions know who to turn to regarding OSS security issues.

Governments should also take stock of the OSS being used and any current OSS security initiatives across various government agencies at the federal and state levels.[66] Ideally, this approach includes an SBOM initiative. Knowing which OSS artifacts are in use by government agencies is an essential precondition for prioritization and follow-on interventions for the Cybersecurity OSPO, as well as for other government OSPOs. Knowing what initiatives and projects exist helps consolidate them by either integrating them into the Cybersecurity OSPO or forming a permanent exchange between them and the Cybersecurity OSPO. Additionally, for the Cybersecurity OSPO to do its job, it would be helpful to know where previous (trusted) relationships exist between the government and various OSS communities.

As an internal coordinator, governments would not have to do everything on their own. Rather, they should serve as a central point for consolidating additional information about various aspects, such as (externally developed) tools for enhancing OSS security, educational resources, and specific guidance on how certain policy provisions would affect the OSS ecosystem from a security standpoint.

[64] Constanze Kurz, Felix Lindner, Frank Rieger and Thorsten Schröder (2008): Derzeitige und zukünftige Auswirkungen der Strafrechtsänderung auf die Computersicherheit and Andrew Crocker (2022): DOJ's New CFAA Policy is a Good Start But Does Not Go Far Enough to Protect Security Researchers

[65] Sven Herpig (2018): Governmental Vulnerability Assessment and Management

[66] Sven Herpig (2022): IT-Sicherheit bei Freier Software: Der Staat ist in der Pflicht

### 3.2.2 Government as a Role Model

*For this role, governments should follow the guidelines of respect, collaboration and sincerity.*

To sustainably foster OSS security, governments should adhere to the community standards, guidelines and best practices that exist in the ecosystem. They have to become role models. Being a role model includes being transparent about all efforts to improve OSS security, to promote the use of secure OSS in any and all government digitization measures and to contribute to better OSS security by sharing vulnerabilities and other security-related information with OSS projects. Being a role model also entails being a responsible OSS consumer, which includes providing notice to OSS project developers when governments discover a vulnerability or develop a patch for their own use.

Additionally, governments must recognize that the OSS ecosystem is inherently international. Maintainers, contributors and other stakeholders in the OSS supply chain of core government OSS projects come from various countries. In addition, stakeholders might operate under pseudonyms with their real identities unknown to the community or to the consumers of their OSS projects. Although this aspect must be acknowledged and considered for further security-related interventions, it should not lead directly to the exclusion of the project from procurement and other processes. Rather, it should mean that governments have at their disposal the right skillset—or trusted third parties with that skillset—to assess the security of OSS. In rare cases, (geo-)political aspects have played a decisive role; for example, the Chinese government has allegedly suddenly restricted access to OSS projects[67], which may (accidentally) negatively impact (large) parts of the OSS ecosystem. Governments should abstain from blocking access, including through sanctions and other measures, to OSS, which includes updated packages and security resources. Doing so would have a detrimental impact on OSS security.

Governments can and should also strive to be role models for other governments and other stakeholders, such as intergovernmental organizations. As a result, others may join the cause for better OSS security. In both ways, especially when cooperation and coordination take place, more resources will be available to improve the security of the OSS ecosystem. The Brno Open Source Declaration[68] is a good example of how an internationalization process can look.

[67] Zeyi Yang (2022): How censoring China's open-source coders might backfire

[68] Otevřená města (2022): Brno Open Source Declaration: The story of the Czech National OSPO

### 3.2.3 Government as a Supporter

*For this role, governments should follow the guidelines of respect, cooperation, collaboration and sincerity.*

While the government's role as an internal coordinator and a role model is focused internally, being a supporter means deliberately and actively using resources to increase security in the OSS ecosystem for all users. As supporters, governments need to engage in capacity building, contribute and provide funding.

There is a range of initiatives and projects that governments can fund to improve the security of the OSS ecosystem. In part, this is because security either is not high on the priority list of many developers, maintainers and contributors[69] or requires additional expert knowledge from a different domain[70]. Although it would be great for this situation to change, as a supporter, the government should share that responsibility and invest in fixing existing shortcomings. This includes, but is not limited to, rewrites of software in memory-safe programming languages[71], security audits[72], vulnerability coordination[73], help with documentation[74], patch reward programs[75] and incident response funds[76].

Governments should carefully evaluate which of these interventions they should implement directly. Existing initiatives and OSS institutions may be better positioned than governments to bridge the gap between government funding processes and (volunteer-based) OSS projects, which may struggle to navigate bureaucratic funding requirements. Therefore, a government should look for existing initiatives, such as the Open Source Software Security Mobilization Plan[77], to see whether they already cover the planned interventions. If so, and if funding them is possible, governments should fund them. If suitable initiatives do not exist, governments can contract third parties with previous experience in the OSS ecosystem and task them with designing and implementing these interventions. This must be done in close

[69] Frank Nagle, David A. Wheeler, Hila Lifshitz-Assaf, Haylee Ham and Jennifer L. Hoffman (2020): Report on the 2020 FOSS Contributor Survey and Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report

[70] Dialog für Cybersicherheit (2023): Log4shell & Consequences

[71] Dan Lorenc (2021): Mitigating Memory Safety Issues in Open Source Software and Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure

[72] Bundesamt für Sicherheit in der Informationstechnik (2015): Sicherheitsanalyse TrueCrypt

[73] Allen D. Householder, Garret Wassermann, Art Manion and Chris King (2017): The CERT® Guide to Coordinated Vulnerability Disclosure and Tassilo Thieme (2021): Heureka! Von der Schwachstellenfindung bis zur Veröffentlichung: Entwicklung eines Coordinated Vulnerability Disclosure Prozesses für kleine und mittelständische IT-Unternehmen

[74] Tidelift (2021): Survey Finds Many Open Source Maintainers Are Stressed Out and Underpaid, But Persist So They Can Make a Positive Impact

[75] Google Bug Hunters (2023): Patch Rewards Program Rules

[76] Open Source Security Foundation (2022): The Linux Foundation and Open Source Software Security Foundation (OpenSSF) Gather Industry and Government Leaders for Open Source Software Security Summit II and Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure

[77] The Linux Foundation and Open Source Security Foundation (2022): The Open Source Software Security Mobilization Plan

coordination with the affected OSS communities and ideally other Cybersecurity OSPO-like entities internationally.

Additionally, governments can provide security resources such as guidelines or tools and, under certain circumstances (such as abandoned critical projects), secure forks or adopt orphaned packages. Moreover, governments can provide support through development resources, such as contributions to third-party open source libraries and releases of open source code. Moreover, through participation, funding or other forms of contribution, governments should support existing community events such as FOSDEM[78], as the European Commission has done in the past[79].

Although it is clear that governments should focus their efforts on OSS components that are *most used by government agencies* or *most used by critical infrastructure*, it is important to coordinate those efforts with other existing initiatives internationally to invest resources efficiently. This requires a strong connection to the international ecosystem and its relevant players. Governments can also help foster an understanding of critical dependencies by releasing data on which OSS components are most depended on by the government and/or critical infrastructure.

### 3.2.4 Government as a Regulator

*As a regulator, governments should follow especially the guidelines of respect, cooperation and sincerity.*

The role of governments as regulators is tricky in the OSS ecosystem. The OSS ecosystem is international; therefore, national regulation faces multiple limitations. Additionally, due to the complexity of the ecosystem, regulating well without stifling innovation or worsening the security situation seems to be particularly challenging, again referring back to the debate surrounding the OSS provisions in the CRA that would shift liability toward individual OSS developers and maintainers, who often cannot support it[80]. This does not mean that governments should avoid regulation directed at the OSS ecosystem at all costs. However, regulation can have a positive effect only if governments improve their understanding of the OSS ecosystem through dialogue and cooperation, and by being extremely nuanced and inclusive in their approach to regulation.

In their role as regulators, governments should abolish barriers for OSS communities. This includes the aforementioned review of protection of security researchers in

[78] FOSDEM team (2023): FOSDEM 2023

[79] FOSDEM team (2023): FOSDEM 2023 - How regulating software for the European market could impact FOSS

[80] See, for example, Maarten Aertsen (2022): Open-source software vs. the proposed Cyber Resilience Act and Aeva Black and Gil Yehuda (2022): Open Source Security Policy Conundrum and Olaf Kolkman (2022): The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem

legal provisions on computer crime[81] as well as public procurement law. Government procurement guidelines have often been developed with private sector applications and proprietary software in mind.[82] Certain provisions, such as expensive certifications, requirements that developers and other stakeholders be citizens (of certain states) or requirements to grant exclusive rights for use of the software (which are incompatible with most OSS licenses by default), strongly discourage or even exclude applications from OSS communities. Changing those conditions and thus enabling OSS communities to better participate in public procurement processes will certainly strengthen the OSS ecosystem and lead, in general, to more competition and better choices for governments when it comes to tenders in which more applicants participate. Facilitating the participation of OSS projects in public procurement will also lead to more funds available to the OSS ecosystem and wider adoption of OSS. Then, OSS security for critical packages can ultimately be fostered through requirements, such as certifications, attestations and/or approvals, in public tenders that are compatible with the OSS approach. Regulation of this form could improve the security of OSS used by governments without overburdening the developers of OSS projects. Reducing barriers will strengthen competition, especially if paired with direct incentives. Such an incentive could be tax credits for contributions to OSS[83], even if money may not always be the top incentive for the stakeholders involved[84].

One area where governments may want to consider regulation that directly affects individual developers and contributors as well as MSMEs are SBOMs. So many government interventions aimed at improving security, tracking vulnerabilities and managing versions and license compliance can be built on SBOMs that it seems prudent to require them—or something similar—at least for product vendors within the next few years. This is an additional burden for those stakeholders, but it seems necessary. Governments should offer support, such as guidelines and tooling, to facilitate the process as much as possible. This can be done in cooperation with intermediaries, such as repositories, to offer the tooling to developers by default during the development process, requiring as little effort from the developers as possible.

[81] Constanze Kurz, Felix Lindner, Frank Rieger and Thorsten Schröder (2008): Derzeitige und zukünftige Auswirkungen der Strafrechtsänderung auf die Computersicherheit and Andrew Crocker (2022): DOJ's New CFAA Policy is a Good Start But Does Not Go Far Enough to Protect Security Researchers

[82] Open Source Business Alliance (2022): Öffentliche Beschaffung von Open Source Software mit EVB-IT vereinfachen

[83] Frank Nagle (2022): Strengthening digital infrastructure: A policy agenda for free and open source software

[84] Tidelift (2021): Survey Finds Many Open Source Maintainers Are Stressed Out and Underpaid, But Persist So They Can Make a Positive Impact and Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report

# 4. A Government Cybersecurity Open Source Program Office

## 4.1 Open Source Program Office

Although governments' roles serve as a guideline, an institutional setup is required for governments to engage with a "patchwork of private and nonprofit efforts"[85] in the OSS space and implement policy interventions for more secure OSS.

OSPOs are a commonly chosen model in industry and other sectors to coordinate all types of open source efforts, not just those related to security.[86] OSPOs are "designed to be the center of competency for an organization's open source operations and structure"[87] and to "foster an open source culture inside the organization [...] from engineering to sales to marketing"[88]. There is no one-size-fits-all model[89], but "a typical OSPO [can be categorized] into three categories: Legal Risk Mitigation, Improving Engineers' Practices and Enabling Financial Benefits"[90]. "This can include setting code use, distribution, selection, auditing and other policies, as well as training developers, ensuring legal compliance and promoting and building community engagement that benefits the organization strategically"[91].

For governments, setting up an OSPO can be the first step to "being a responsible OSS consumer"[92]. These government OSPOs may be tasked with "project support, license compliance, security evaluation, incident response, public awareness, and providing clear points of contact for government employees and OSS developer[s]"[93] as well as with "coordinat[ing] federal policies related to FOSS [Free and Open Source Software]"[94]. Established or planned government OSPOs[95] include the European EC

[85] Trey Herr, Robert Morgus, Stewart Scott and Tianjiu Zuo (2022): Buying down risk: Open source software
[86] Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure
[87] Chris Aniszczyk, Gil Yehuda and Tulio Leao (2022): Open Source Program Office (OSPO) Definition and Guide
[88] Brian Proffitt (2019): What does an open source program office do?
[89] Jeff McAffer quoted in Chris Aniszczyk, Jeff McAffer, Will Norris, Andrew Spyker and Remy DeCausemaker (2022): How to create an open source program office
[90] Chris Aniszczyk, Gil Yehuda and Tulio Leao (2022): Open Source Program Office (OSPO) Definition and Guide
[91] Chris Aniszczyk, Gil Yehuda and Tulio Leao (2022): Open Source Program Office (OSPO) Definition and Guide
[92] Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure
[93] Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure
[94] Frank Nagle (2022): Strengthening digital infrastructure: A policy agenda for free and open source software
[95] For case studies of government OSPOs, see OpenForum Europe and The OSPO Alliance (2022): The OSPO - A New Tool for Digital Government

OSPO[96], the OSPO of the World Health Organization (WHO)[97], the French OSPO[98] and the Czech national OSPO[99]. With "a trend toward establishing Open Source Programs Offices (OSPOs) in government organizations"[100] and "the public sector [as] an area of rapid policy innovation"[101], it is expected that governments may set up several OSPOs to serve different functions related to government OSS.[102] These OSPOs "should be an enabler" and not "an additional bureaucratic layer"[103].

Cybersecurity, similar to OSS, is a complex ecosystem for which governments have created specific agencies that are tied into the security, defense and intelligence domains. As incidents have shown over the years, government efforts for OSS should focus on, among other topics, security. Additionally, these efforts should be integrated with government supply chain security[104] approaches. Relatedly, operations targeting OSS have shown that incident response is a crucial topic at the intersection of cybersecurity and OSS, requiring a "focal point for operational efforts"[105]. Given the intersections of cybersecurity and OSS, governments' genuine interest and existing resources in (cyber)security, and the prospect of multiple OSPOs per country, this paper pursues the idea of a Cybersecurity OSPO.

## 4.2 Institutional Setup

Acknowledging that other OSPOs may be based in various parts of the government architecture, a Cybersecurity OSPO could start out as a task force or unit within the national cybersecurity agency[106]. Based there, the Cybersecurity OSPO could be a "source of support and advocacy for open source security as a component of supply-chain security policy work, coordinating across government agencies and offices to ensure that open source security is no longer tied to a crisis cycle"[107].

[96] European Commission (2020): EC Open Source Programme Office and OpenForum Europe and The OSPO Alliance (2022): The OSPO - A New Tool for Digital Government

[97] Astor Nummelin Carlberg (2022): The WHO is the latest public administration to launch an Open Source Programme Office

[98] Paulina Grzegorzewska (2021): French Minister announces new plan for supporting open source and OpenForum Europe and The OSPO Alliance (2022): The OSPO - A New Tool for Digital Government

[99] Otevřená města (2022): Brno Open Source Declaration: The story of the Czech National OSPO

[100] Mike Linksvayer (2022): The changing nature of governmental policies around open source

[101] OpenForum Europe and The OSPO Alliance (2022): The OSPO - A New Tool for Digital Government

[102] Frank Nagle (2022): Strengthening digital infrastructure: A policy agenda for free and open source software and Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure

[103] OpenForum Europe and The OSPO Alliance (2022): The OSPO - A New Tool for Digital Government

[104] Alexandra Paulus and Christina Rupp (2023): Government's Role in Increasing Software Supply Chain Security and Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure and Trey Herr, Robert Morgus, Stewart Scott and Tianjiu Zuo (2022): Buying down risk: Open source software

[105] Trey Herr, Robert Morgus, Stewart Scott and Tianjiu Zuo (2022): Buying down risk: Open source software

[106] Trey Herr, Robert Morgus, Stewart Scott, and Tianjiu Zuo suggested to create such an office for the United States at the Cybersecurity and Infrastructure Security Agency (CISA) in Trey Herr, Robert Morgus, Stewart Scott and Tianjiu Zuo (2022): Buying down risk: Open source software. The Linux Foundation describes various OSPO structures in Ibrahim Haddad (2022): A Deep Dive Into Open Source Program Offices - Structure, Roles, Responsibilities, and Challenges.

[107] Trey Herr, Robert Morgus, Stewart Scott and Tianjiu Zuo (2022): Buying down risk: Open source software

Setting up the Cybersecurity OSPO within the national cybersecurity agency has several advantages. First, it can leverage existing intersections between the government's cybersecurity efforts and its use of OSS, including its role as an OSS consumer, as well as its points of contact and advocates for OSS. Additionally, it brings the needed security mindset into the Cybersecurity OSPO. Moreover, it allows direct access to processes such as standardization working groups and incident response mechanisms. Therefore, OSS security efforts need to address all stages, from prevention to detection and response. This can be covered comprehensively by a national cybersecurity agency that taps into the national security ecosystem.

The downside of having the Cybersecurity OSPO tied to the national cybersecurity agency is that security equity will always be weighed heavier than other equities, such as innovation. However, that is the role of a Cybersecurity OSPO and can be balanced by other OSPOs with different focuses across the government. Another disadvantage is the proximity to the national security ecosystem, which may alienate OSS communities. To prevent this, the Cybersecurity OSPO ideally is not housed in agencies that are responsible for signals intelligence, intrusive cyber operations or similar activities. Additionally, the Cybersecurity OSPO must heavily invest its resources and provide benefits to the OSS ecosystem. The Cybersecurity OSPO's role as a supporter must be emphasized. Trust must be earned, and the ball is—and may always be—in the Cybersecurity OSPO's court.

However, the Cybersecurity OSPO does not need to implement all OSS security efforts on its own. A large part of its job is to advise government efforts across stakeholders. Larger research projects on OSS security may be run by research and innovation agencies such as the American DARPA[108] and the German Cyberagentur[109]. Government funding for security-related OSS projects may come from or through stakeholders such as the Sovereign Tech Fund[110]. Policies covering OSS (security)-related provisions also do not originate from within the national cybersecurity agency. Therefore, while implementing certain OSS security-related efforts by the government, especially at the operational level, the agency will have a strong advisory role in all other efforts. The efforts of other stakeholders within the government ecosystem can also help address any gaps in trust or other areas where the national cybersecurity agency's Cybersecurity OSPO may fall short. Independent of whether the Cybersecurity OSPO implements interventions itself or advises other stakeholders regarding their interventions for

[108] Defense Advanced Research Projects Agency (2023): Creating Breakthrough Technologies And Capabilities For National Security
[109] Agentur für Innovation in der Cybersicherheit GmbH (2023): Aktuelles
[110] Sovereign Tech Fund (2023): Stärkung von digitalen Infrastrukturen und Open-Source-Ökosystemen im öffentlichen Interesse

OSS security, a Cybersecurity OSPO needs staff with the right competencies[111] and ideally, previous trusted relationships with OSS communities.[112]

## 4.3 Policy Interventions[113]

### 4.3.1 General Interventions

Government efforts, including those of the Cybersecurity OSPO, must make OSS more secure. Acknowledging that software will always be insecure to a certain extent, policy interventions should cover the entire spectrum, ranging from prevention to detection and reaction to security incidents. The mindset driving the Cybersecurity OSPO should be to make OSS more secure while at the same time enabling OSS developers to innovate and OSS consumers to become more resilient. Although policy interventions may emphasize the beginning of the software lifecycle, such as development, continuous integration and delivery to improve security of future OSS, existing OSS cannot be neglected. The starting point is a world with a wide range of insecure software; thus, post-deployment and end-of-life interventions are key to securing what is widely used. The following interventions cannot and should not be conducted in a vacuum. **Wherever possible, governments should leverage partnerships, for example, with other governments—ideally their Cybersecurity OSPOs—to increase the effectiveness of the interventions and avoid duplicating efforts.** Before providing specific policy interventions against the backdrop of the software development lifecycle, the Cybersecurity OSPO may want to consider general policy interventions.

First, the Cybersecurity OSPO needs to **drive stocktaking of the government's inventory** of all OSS used throughout the software stack for the government information technology enterprise and its nation's critical infrastructure. Several follow-up actions, such as effective information sharing, depend on this. More importantly, all prioritization involved in OSS security policy interventions depends on this. The scope may be extended to critical infrastructures and other sectors of vital importance to national security. As a by-product of the stocktaking, the Cybersecurity OSPO could **provide software repositories of vetted versions of OSS that are used by government agencies**.

Second, the Cybersecurity OSPO should **create an information portal**, or simply an **OSS security landing page,** as an extension for existing portals, to provide and link all resources for improving OSS security (best practices, guidelines, contact addresses for OSS security teams, etc.) as well as related threat intelligence and incidents.

[111] For more information about OSPO staffing, see Ibrahim Haddad (2022): A Deep Dive Into Open Source Program Offices - Structure, Roles, Responsibilities, and Challenges.
[112] For further details, see 4.4.2 Capabilities and 4.4.3 Credibility under 4.4 Resource Mobilization.
[113] For a full list of policy interventions, see Annex B.

Ideally, this portal should be easily accessible and written in English and in the national language. Many materials are available only in English; governments may wish to fund efforts (possibly pooling them) to ensure that materials are available and maintained in other languages to maximize their application. The portal should primarily reference existing sources to provide a one-stop shop for all matters of OSS security.

Third, the Cybersecurity OSPO should **advise legislative and executive branches** on legislation and policies that have an impact on OSS security. The Cybersecurity OSPO should also proactively raise issues, such as a review of the OSS compatibility of current procurement law and computer crime laws hacking.

Fourth, the Cybersecurity OSPO should **support OSS security-relevant initiatives, infrastructure and tools.** Although funding will be the main tool to drive this policy intervention, other contributions, as well as echoing the message, will also be useful.

Fifth, the Cybersecurity OSPO should **actively engage in education** on OSS security for all stages of life and career in cooperation with existing institutions and actors such as universities, non-government organizations, training centers and influencers. This education should include support during all stages of formal education, as well as training and certifications for developers and contributors. Currently, software developers often are not taught how to develop secure software. Additionally, the Cybersecurity OSPO should **support research** on all matters of OSS security, including technical and policy issues.

Finally, the Cybersecurity OSPO needs to **engage with the OSS ecosystem** and **advocate for OSS communities.** Under certain conditions, for example, during public procurement or vulnerability disclosure, OSS communities may need an intermediary. The Cybersecurity OSPO is well suited for that task. To remain attuned to the OSS ecosystem and raise awareness of OSS security within and outside the government, the Cybersecurity OSPO should regularly **exercise its convening power**.

### 4.3.2 Interventions During Development

The development of software is when security can most easily be baked into software. However, the Cybersecurity OSPO will not be able to have a significant direct impact on projects at this point and should instead promote OSS security guidance and/or education. The Cybersecurity OSPO can **work toward better education on secure software development, provide corresponding guidelines for software developers, offer fellowships for secure software development, fund the development of developer security tools and encourage the use of memory-safe programming languages**. Additionally, the Cybersecurity OSPO can strengthen the framework for development, for example, by **harmonizing existing concepts,** such as software development lifecycle models. In terms of more direct support, the Cybersecurity OSPO could **fund code-level security audits**.

Policy interventions at this point will likely come in the form of supporting existing initiatives by industry and non-government organizations. However, three concrete actions can be taken directly by the Cybersecurity OSPO: **creating an information portal on all resources for secure software development**, **actively promoting OSS security interest in standardization working groups** (including financial incentives for seconded experts) and **supporting (including teaching) curricula that focus on secure software development**.

### 4.3.3 Interventions During Continuous Integration and Delivery

In software development, third-party infrastructures, such as repositories[114], and tools for integration[115] and corresponding security checks[116] play a major role. Following a shared responsibility model, infrastructure providers are responsible for their own security. Additionally, there are initiatives aimed at improving existing tooling, providing additional tools and running tools on selected OSS.[117]

There are several actions that the Cybersecurity OSPO can take at this point. First, it can **add existing, vetted, security-related resources about tooling and infrastructure to the information portal**. Current security advisories regarding tooling and infrastructure should be shown, as well as past incidents, for example, Gitee censorship[118].

**The Cybersecurity OSPO could support tooling and infrastructure providers through funding (directly or indirectly through third parties) or by providing threat intelligence**[119]. Additionally, the Cybersecurity OSPO could use incentives, such as naming and shaming, to **nudge the security posture of providers** and to implement mandatory two-factor authentication for repository infrastructure providers, for example[120].

Finally, the Cybersecurity OSPO could **provide its own infrastructure**, such as a repository[121], and **share tools the government is using** to improve the security of its software. Again, it is more advisable to support existing initiatives and tooling rather

[114] For example, Github or Gitee
[115] Max Rehkopf (2023): Continuous integration tools
[116] For example, tests and audits to verify commits and merges, vetting of third-party code in the software stack, security checks in the build and signing processes, and dynamic and static analyses.
[117] For example, the Open Source Security Foundation
[118] Zeyi Yang (2022): How censoring China's open-source coders might backfire
[119] Zoë Brammer, Silas Cutler, Marc Rogers and Megan Stifel (2023): Castles Built On Sand - Towards Securing The Open-Source Software Ecosystem
[120] Laura Paine and Hirsch Singhal (2023): Raising the bar for software security: GitHub 2FA begins March 13
[121] Germany set up its own exclusive repository for public administration OSS projects, see Der Beauftragte der Bundesregierung für Informationstechnik (2022): Open CoDE - Open Source-Plattform der Öffentlichen Verwaltung

than create something from scratch whenever possible and feasible. Should there be existing tools within the government, they could be provided to the public.

### 4.3.4 Interventions Post-Deployment

Interventions during post-deployment are almost entirely focused on ensuring that existing bugs are found and that information about them is sent upstream for fixing and downstream for awareness. Compared to earlier parts of the software development lifecycle, the Cybersecurity OSPO can be especially active with its interventions here.

Bugs in deployed software can be found by various entities for many reasons. They include security researchers for fun or bounties, developers of OSS and proprietary software integrating software artifacts into their own code, and intelligence agencies and companies providing offensive and surveillance tools to governments and others. Bugs found in OSS should be communicated upstream to developers and contributors, for example, through communication channels, such as bug-tracking platforms[122]. The developers then provide a bugfix in the form of a patch and inform software using entities downstream that they need to update this OSS package. This process poses several challenges that the Cybersecurity OSPO could step in to help. Additionally, the Cybersecurity OSPO could support finding and distributing information about mitigation mechanisms until a patch is distributed.

First, the Cybersecurity OSPO can **provide incentives to find bugs**. Although OSS security generally benefits from Linus' Law, namely, "given enough eyeballs, all bugs are shallow"[123], about 40% of the top OSS packages analyzed have 5 or fewer developers[124]. A Cybersecurity OSPO could, for example, coordinate or fund a patch bounty or commission security audits. In both cases, **assessing the most critical OSS projects from the Cybersecurity OSPO's perspective** first and deriving prioritization and therefore scope from it are important bases for these activities. As discussed below, bug bounty programs and security audits should be paired with incentives and support for fixing bugs; otherwise, OSS projects may end up with a high number of low-priority bugs that take up already scarce resources. Additionally, the Cybersecurity OSPO could **facilitate (transborder) vulnerability reporting**[125] through issuing guidelines for developers on the information portal, offering itself as a coordinator and supporting similar efforts by the developer platforms.

[122] Alex Ivanovs (2021): The 15 Best Bug Tracking Platforms for Developers
[123] Eric Steven Raymond (2000): The Cathedral and the Bazaar
[124] Basis: The first 10% of 6,592,414 packages in the Ecosyste.ms dataset (which excludes removed packages) by average ranking, which is a combination score made up of relative downloads, dependent packages, dependent repos, stars and forks for each ecosystem. Excluded were ecosystems where the API does not provide data on the number of maintainers.
[125] Alexandra Paulus and Christina Rupp (2023): Government's Role in Increasing Software Supply Chain Security

Second, the Cybersecurity OSPO can encourage stakeholders to report found bugs. Interventions range from lowering existing barriers, such as **changes in computer crime laws**[126], to **providing a credible framework for a coordinated vulnerability disclosure process**[127] in which the Cybersecurity OSPO will assist with disclosures. Of course, the Cybersecurity OSPO could also discourage the withholding of information about found bugs, for example, through the **naming and shaming of vendors who fix third-party code in their software stack without reporting it upstream**. Identifying these instances, however, would require automation to scale up.

Third, the Cybersecurity OSPO can provide positive incentives to patch bugs. For security researchers, the Cybersecurity OSPO could **provide a patch reward** so that instead of only reporting a bug, they also include a patch as mentioned earlier. Developers could, for example, receive **tax credits for their time working on OSS**. Again, positive and negative incentives that **nudge third-party developers to reshare improved code** should also be on the table. The Cybersecurity OSPO could also **commission a patch, secure fork or rewrite of an OSS component.**

Fourth, the Cybersecurity OSPO can **facilitate information sharing across stakeholders by supporting core projects,** such as the SBOM[128], Common Vulnerabilities and Exposures (CVE)[129], Vulnerability Exploitability eXchange (VEX)[130] or the Common Security Advisory Framework (CSAF)[131]. A SBOM helps understand what the software stack is composed of,  CVE identifies the publicly known vulnerabilities (and in what components), VEX contains information on whether vulnerabilities in the software stack are exploitable and CSAF enables automation for finding, evaluating and implementing security advisories. In this way, information about vulnerabilities and patches can be communicated more effectively downstream to reach affected parties. As many follow-up activities hinge on information about the software stack, the Cybersecurity OSPO may, if adoption rates remain low, advocate for stronger negative incentives. However, negative incentives should always be the last resort.

### 4.3.5 Interventions at End-of-Life

The end-of-life (EOL) is the stage in which a Cybersecurity OSPO might be most proactive. EOL generally means that a project (OSS or not) is no longer maintained.

[126] Constanze Kurz, Felix Lindner, Frank Rieger and Thorsten Schröder (2008): Derzeitige und zukünftige Auswirkungen der Strafrechtsänderung auf die Computersicherheit and Andrew Crocker (2022): DOJ's New CFAA Policy is a Good Start But Does Not Go Far Enough to Protect Security Researchers

[127] Cybersecurity & Infrastructure Security Agency (2023): Coordinated Vulnerability Disclosure Process and European Union Agency for Cybersecurity (2022): Coordinated Vulnerability Disclosure policies in the EU

[128] Cybersecurity And Infrastructure Security Agency (2023): Software Bill of Materials (SBOM)

[129] The MITRE Corporation (2023): Overview - About the CVE Program

[130] Cybersecurity & Infrastructure Security Agency (2022): Vulnerability Exploitability eXchange (VEX) – Use Cases

[131] Bundesamt für Sicherheit in der Informationstechnik (2023): Common Security Advisory Framework (CSAF)

However, although triggers and definitions may exist for different OSS communities[132], there is no general rule for when an OSS project is considered "no longer maintained". **Identifying and mapping this for different OSS communities may be a good starting point for the Cybersecurity OSPO.**

With the project community, developers and contributors out of the picture, there may be no central stakeholder that can maintain the project and care for its security. Although developers and contributors do take over projects from other communities, only about 40% of the top OSS packages have had a release within the past two years[133]. Thus, bugs found in those OSS components may have nowhere to be reported to and therefore will not be fixed. Additionally, although the dependencies that OSS components rely on may be updated without maintenance, they will still be pulling in outdated dependencies.

The Cybersecurity OSPO should **offer guidelines for software recycling and responsible sunsetting**. Additionally, the Cybersecurity OSPO should point toward or even **support existing adopt-a-package initiatives**[134]. Moreover, it should assess the potential needs of existing end-of-life platforms[135] and, if all else fails, **serve as a point of contact for OSS project communities abandoning their projects**.

For orphaned OSS projects within the scope of prioritization (e.g., used in a government or critical infrastructure software stack), the Cybersecurity OSPO may want to **alert downstream users about end-of-life dependencies** and **commission patches, rewrites or secure forks** when bugs or vulnerabilities are reported. Although funding is one of the main policy interventions across the software development lifecycle, the Cybersecurity OSPO may need a **dedicated "troubleshooting" fund** that will be used for commissioning patches, rewrites and forks during post-deployment and at EOL.

## 4.4 Resource Mobilization

### 4.4.1 Funds

Funds are needed to implement a variety, likely most, of governments' policy interventions. Funding is especially needed to fulfill the government's role as a

[132] The Apache Software Foundation, for example, considers Apache projects a good candidate for the Attic platform, and therefore, at the end of life, when "PMC [Project Management Committee] are unable to muster 3 votes for a release, who have no active committers or are unable to fulfill their reporting duties to the board", The Apache Software Foundation (2023): The Apache Attic

[133] Basis: The first 10% of 6,592,414 packages in the Ecosyste.ms dataset (which excludes removed packages) by average ranking, which is a combination score made up of relative downloads, dependent packages, dependent repos, stars and forks for each ecosystem.

[134] Stewart Scott, Sara Ann Brackett, Trey Herr, Maia Hamin with the Open Source Policy Network (2023): Avoiding the success trap: Toward policy for open-source software as infrastructure

[135] An example of such platforms is the self-sustainable Apache Attic, see The Apache Software Foundation (2023): The Apache Attic

supporter. Core funding and staffing should be provided by the institution to which the Cybersecurity OSPO is connected. According to the points raised earlier, the national cybersecurity agency is a potential candidate.

As the Cybersecurity OSPO does not necessarily have to implement the aforementioned policy interventions itself but can also coordinate their implementation, funds can be either transferred to the Cybersecurity OSPO and be managed there or spent by other stakeholders under (loose) coordination of the Cybersecurity OSPO. One set of stakeholders that should allocate funds for improved OSS security is government agencies using OSS. This could, for example, be realized by a **government OSS security dividend**[136] based on OSS usage that follows the OSS stocktaking.

Additionally, companies using OSS—either as consumers or in their software stacks—should allocate funds for OSS security. To better coordinate spending, the Cybersecurity OSPO could form a **focal public–private partnership in which the Cybersecurity OSPO steers the pledged investment from companies** to the needed policy interventions, including funding of operational security initiatives such as code-level security audits and rewrites.

In a similar manner, the Cybersecurity OSPO should **connect to existing networks, research agencies and dedicated funds**, such as the European Cybersecurity Competence Centre and Network[137] and the Sovereign Tech Fund, to leverage the funds from those stakeholders for policy interventions for OSS security.

While ideally the Cybersecurity OSPO is equipped with enough funding to implement the needed policy interventions, it can and should leverage existing and mobilize additional funding from the public and private sectors. **This funding can then be spent either through the Cybersecurity OSPO or directly by the stakeholders, with coordination by the Cybersecurity OSPO.**

Relatedly, a lighter touch by the Cybersecurity OSPO could be **brokering between companies that would like to invest in OSS security and OSS projects that need funding.** Additionally, the Cybersecurity OSPO could **help OSS project teams apply for grants** or other forms of funding, for example, by leveraging existing national and international connections and access to funders.

No matter where the funding comes from or whether the Cybersecurity OSPO is directly funding an initiative or coordinating the funding of another government entity, one core rule must be followed: **minimize the strings attached.** Accountability frameworks dictate how governments can spend money and monitor compliance, but the Cybersecurity OSPO should aim to minimize requirements for the recipients

[136] Sven Herpig (2022): IT-Sicherheit bei Freier Software: Der Staat ist in der Pflicht
[137] European Cybersecurity Competence Centre (2023): European Cybersecurity Competence Centre and Network

of the funding, especially if they are individuals or MSMEs, as much as possible. This approach reduces the burden placed on those entities and therefore creates better incentives to apply for funding to improve the security of their projects.

### 4.4.2 Capabilities

Having capabilities and knowledge surrounding OSS security is crucial to being an internal coordinator, a role model and an effective regulator. Capabilities are at the heart of getting policy interventions right.

However, most OSS security capabilities will likely be found outside the government. Individuals with these skills are unlikely to switch careers or join the government for this purpose alone. Therefore, the Cybersecurity OSPO has to define what capabilities are needed and then explore ideas on how to **temporarily leverage outside resources and channel them toward good policy interventions and internal capacity building**. This can be done in a number of ways, such as offering paid **fellowships**[138] or creating an **advisory board** with paid positions for representatives from civil society and research. Emphasizing outside support will also lead to a stronger engagement with the OSS ecosystem, which, by all means, can only be beneficial for the Cybersecurity OSPO and government.

To effectively leverage external resources, however, the Cybersecurity OSPO needs a core staff with relevant capabilities. Therefore, the organization should **bring together existing capabilities** within which it is set up. Additionally, it should map **existing capabilities across the government.** Given the current shortage of skilled IT security staff, making effective use of existing resources is crucial. External government staff with OSS security capabilities could be connected to the Cybersecurity OSPO, for example, through a liaison program, an interagency task force or simply ad hoc meetings on relevant topics. To enhance the capabilities of the Cybersecurity OSPO's native staff and those on loan from other government stakeholders, the organization should prioritize **incentivizing capacity building** through training and participation in conferences. Furthermore, the staff should be empowered and encouraged to devote their work hours to contributing to OSS projects, particularly those that are relevant to security.

### 4.4.3 Credibility

To be effective in improving OSS security within the ecosystem, credibility and trust within OSS communities is vital. Credibility and trust are defined by past actions; therefore, a long-term and steady commitment by the government is crucial. Credibility is required for governments to be effective supporters, as this role relies heavily on cooperation from OSS communities. For this cooperation to work and

[138] See, for example, SPD/Volt-Stadtratsfraktion (2023): Open Source Sabbatical in München startet

build credibility, governments need competent staff. At the same time, this role is designed to build credibility and trust within communities.

Although there are likely trusted personal relationships between government staff and individuals in the OSS ecosystem, it is best to assume that institutional relationships are not personal. Therefore, most governments are likely to start at zero and earn trust and credibility first. Governments start their journey to become OSS security champions by being internal coordinators and later role models. In these roles, the Cybersecurity OSPO should **proactively and clearly explain its role and manage expectations.**

The Cybersecurity OSPO should additionally **identify existing relationships** at the operational and strategic levels to explore whether government staff would be willing to use their positions within the OSS ecosystem to serve as advocates and bridge-builders between the government and the OSS ecosystem. These ties should be strengthened and extended through **participation in and support of community events and conferences, offering OSS security resources free of charge,** and **joining existing efforts** to improve the OSS ecosystem.

Regarding communication, the idea of **reciprocity** should permeate all interactions. The Cybersecurity OSPO must ensure that OSS communities' information sharing about security issues with the government is not a one-way street.

Finally, it is the Cybersecurity OSPO's responsibility to **leave no one behind.** Therefore, it should extend its scope towards cooperation with smaller projects and MSMEs. Larger projects and companies may already be addressed by other initiatives, but as a real champion for OSS security, the Cybersecurity OSPO should direct its attention (and resources) to the groups that are otherwise easily forgotten.

## 5. First Steps

After getting a better idea of the possible roles of governments for fostering OSS security and the underlying guidelines, the previous section made suggestions for the concrete setup, interventions and resources of a Cybersecurity OSPO. This section outlines the first steps of how governments can contribute to a policy environment that enables a Cybersecurity OSPO to thrive and effectively assume its role in the OSS ecosystem. However, an important precondition is that a government has shown an awareness of and genuine interest in OSS. For example, Germany has signaled this by including OSS in its policy plan ("coalition agreement")[139] and digital strategy[140] for the current legislative term. Without that kind of traction, it would be difficult to push toward securing OSS. If there is some momentum for OSS and security in the current political landscape, these are the first steps governments[141] can take to build trust and create real value for the community. The Cybersecurity OSPO can then mature over time.[142] The first steps governments may take towards their own Cybersecurity OSPO are:

**Have clear goals:** As the first step, governments need to identify their OSS goals before building the Cybersecurity OSPO to achieve them.[143] Interventions by the organization should follow a concrete plan that outlines the goals for the next 3 to 5 years but includes several "easy wins" for the first year of existence. Thus, governments should publish an OSS cybersecurity agenda and equip the Cybersecurity OSPO with the means to implement the agenda.

**Do it right from the beginning:** The initiative should adhere to the principles of the OSS ecosystem from the get-go. This means that the basis for all future work of the Cybersecurity OSPO (e.g., the mission statement) should be informed by an open development process.

**Just do it:** A Cybersecurity OSPO does not necessarily require setting up a new agency. If it is understood as a platform, it can be set up within an existing agency or OSPO and therefore has an extremely low entry barrier. However, the Cybersecurity OSPO needs the maximum degree of flexibility and independence from the agency to be effective. For example, an internal agency task force could be done tomorrow. Another

[139] Sozialdemokratische Partei Deutschlands (SPD), Bündnis 90 / Die Grünen und Freie Demokraten (FDP) (2021): Mehr Fortschritt wagen
[140] Federal Ministry for Digital and Transport (2022): Digitalstrategie
[141] Currently, the following governments may have sufficient traction in this direction: the United States, Germany, the Netherlands, France and Czech Republic, as well as the European Commission.
[142] For OSPO maturity levels, see The Linux Foundation (2022): A Deep Dive Into Open Source Program Offices - Structure, Roles, Responsibilities, and Challenges
[143] OpenForum Europe and The OSPO Alliance (2022): The OSPO - A New Tool for Digital Government

starting point is hiring an “Open Source Software Security Lead to collaborate with the OSS community and Federal partners to secure the OSS ecosystem”[144].

**Start small but effectively:** A small, dedicated group is all that is needed to start the process. Ideally, this group includes agency staff with OSS expertise and connections as well as a senior decision-maker to drive the process through the hierarchy as smoothly as possible. A major task for this group is to earn and build a reputation among OSS communities; therefore, the right composition and choice of staff are crucial.

**Take your commitments seriously:** To be effective, governments have to show that they take the issue seriously. Therefore, they need to raise awareness of the topic, support Cybersecurity OSPO policy interventions and consider its advice, for example, regarding new policies or reviews of the existing legal framework.

**Don’t get weird:** The OSS ecosystem may be different from what governments are used to. This includes required procurement frameworks as well as international, pseudonymous contributors to projects in core government infrastructure. Ensure that the Cybersecurity OSPO understands the ecosystem and acts in the best interest of OSS security.

**Support with regulation:** Consider regulation that does not burden individual developer communities but helps the Cybersecurity OSPO implement or coordinate its policy interventions. Ideally, this applies as soon as the Cybersecurity OSPO is fully operational, so that it can consult with communities and users. Areas that should be covered are mandatory OSS inventories for government agencies and critical infrastructures, mandatory OSS support contracts for all OSS used by government agencies and critical infrastructures, and the adaptation of computer crime laws.

**Get evaluated:** Although the Cybersecurity OSPO will be part of the government, its purpose is to improve OSS security across the board. As outlined, OSS communities are an integral part of that effort. Therefore, the Cybersecurity OSPO should have its work regularly evaluated by OSS users and OSS communities and adapt accordingly.

[144] Cybersecurity and Infrastructure Security Agency [on Twitter] (2023): We’re hiring an Open Source Software Security Lead [...]

# 6. Conclusion

It is good to see that governments around the world are becoming more serious about contributing to OSS security. However, governments have to acknowledge that it is not just about disjointed policy interventions to score political points because supporting OSS is what governments should do these days. It is in the government's own best interest—and in that of the nation it serves—to strategically invest resources and implement policy interventions to improve the status quo of OSS security in the short *and* long term. The approach must be sustainable. Government agencies and other stakeholders vital to national security, such as critical infrastructures, rely heavily on OSS code. This makes up a large part of the software stack running on their IT systems. The more vulnerable OSS code is, the more likely these stakeholders will be disrupted, spied on and sabotaged—ultimately, endangering national security.

Therefore, it is crucial for governments to determine their role in the OSS ecosystem and contribute to its security. The right role and behavior are not only about regulation and the exact structure of a new office but also involve elements of work and culture as well as issues of trust, and finding a common language to be able to communicate across different institutional settings. This is why finding the right approach is a delicate undertaking that requires tact and sensitivity. This can only be done in cooperation with other stakeholders in the OSS ecosystem.

To ensure that government efforts for more secure OSS are coherent, effective and overall sustainable, governments should set up an Open Source Program Office dedicated to cybersecurity—a Cybersecurity OSPO.

The Cybersecurity OSPO will likely walk a thin line between stakeholders in the OSS ecosystem that do not welcome government intervention in the space and governments that do not see why they should cater to the specific needs of OSS communities. This is, in a nutshell, the Cybersecurity OSPO's most important task: to build that bridge and effectively leverage government resources and tools in cooperation and coordination with other stakeholders in the OSS ecosystem to foster OSS security.

If done right, governments can be strong allies in the endeavor for a more secure OSS ecosystem. And for the governments, that would in turn mean better cybersecurity of its agencies, critical infrastructures, economy and society. Hence, a vital contribution to national security.

# Annex

## A. Security Metrics

| Metric | Category | Scope | Source | Year |
|---|---|---|---|---|
| From 2010 to 2021, there were at least 42 supply chain attacks or vulnerability disclosures involving OSS projects and repositories | Vulnerabilities | Breaking Trust Dataset covering 160+ incidents since 2010 | Trey Herr, Nancy Messieh, June Lee, Will Loomis and Stewart Scott (2021): Breaking trust: The dataset | 2021 |
| 29% of the 10% most popular OSS projects contained at least one known security vulnerability[145] | Vulnerabilities | 3 million Java, JavaScript, Python and .NET projects | sonatype (2021): 2021 State of the Software Supply Chain | 2021 |
| 10.4% of the OSS components downloaded had one or more known vulnerabilities | Vulnerabilities | Java components downloaded from the Central Repository | sonatype (2020): 2020 State of the Software Supply Chain | 2019 |
| Applications[146] have 5.1 outstanding critical vulnerabilities, on average | Vulnerabilities | 1.3 million Java, JavaScript, Python, Go and .NET projects | Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software | 2022 |
| 48% of codebases contained high-risk vulnerabilities[147] | Vulnerabilities | Black Duck Audit of 1,481 codebases[148] | Synopsys (2023): Open Source Security And Risk Analysis Report | 2023 |

[145] Context from the report: "These findings indicate that the vast majority of security research (blackhat and whitehat) is focused on finding and reporting vulnerabilities in projects that are most commonly utilized", sonatype (2021): 2021 State of the Software Supply Chain

[146] Context from the report: "This data was gathered from the use of Snyk Open Source, a static code analysis (SCA) tool", Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software

[147] Context from the report: "High-risk vulnerabilities are those that have been actively exploited, already have documented proof-of-concept exploits, or are classified as remote code execution vulnerabilities." and "Customers can opt out of the vulnerability / operational risk assessment portion of the audit at their discretion", Synopsys (2023): Open Source Security And Risk Analysis Report

[148] Before opt-out, the audit included 1,703 codebases, of which 96% contained open source, Synopsys (2023): Open Source Security And Risk Analysis Report

| Metric | Category | Scope | Source | Year |
|---|---|---|---|---|
| It took 97.8 days, on average, to fix a vulnerability in an application[149] | Vulnerabilities | 1.3 million Java, JavaScript, Python, Go and .NET projects | Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software | 2022 |
| 25% of OSS libraries had unfixed vulnerabilities that are being exploited in the wild | Vulnerabilities | Veracode scanning platform database with 351,000+ unique external libraries in JavaScript, Ruby, Java, PHP, .NET, Python, Go and Swift | VERACODE (2020): State of Software Security: Open Source Edition | 2020 |
| 51% of maintainers do not provide fixes and recommendations for vulnerabilities | Vulnerabilities | 280 survey respondents[150] | Tidelift (2023): The 2023 Tidelift State oOf The Open Source Maintainer Report | 2023 |
| 5% of codebases still contained a vulnerable version of Log4J in February 2023 | Vulnerabilities | Black Duck Audit of 1.481 codebases[151] | Synopsys (2023): Open Source Security And Risk Analysis Report | 2023 |
| 34% of daily Log4j downloads still used vulnerable versions as of March 2023 | Vulnerabilities | Overview provided by a member of the Log4j project | Dialog für Cybersicherheit (2023): Log4shell & Consequences | 2023 |

[149] Context from the report: “While some maintainers might be able to fix vulnerabilities in days or hours, there have been a few vulnerabilities that took years to remediate. We expect that popularity and awareness influence the time to fix. A popular project is more likely to attract other collaborators, and additional collaborators can speed up incident response time. In addition, if a project is popular, awareness by users (including via technical press news) is likely to be larger”, Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software

[150] “Participants were contacted via Tidelift’s email lists and social media in November and December 2022”. Data is based on “339 respondents who a) maintain at least one open source project and b) completed a majority of the questions”, Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report

[151] Before opt-out, the audit included 1,703 codebases, of which 96% contained open source, Synopsys (2023): Open Source Security And Risk Analysis Report

| Metric | Category | Scope | Source | Year |
|---|---|---|---|---|
| 96% of software products include at least some OSS component | Dependencies | Black Duck Audit of 1,703 codebases | Synopsys (2023): Open Source Security And Risk Analysis Report | 2023 |
| OSS projects have, on average, 68.8 dependencies[152] | Dependencies | 1.3 million Java, JavaScript, Python, Go, and .NET projects | Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software | 2022 |
| 24% of organizations are confident in the security of their direct dependencies | Dependencies | 539 small, medium and large organizations[153] (margin of error is +/- 3.6% at the 90% confidence level) | Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software | 2022 |
| 18% of organizations are confident in the security of their transitive dependencies | Dependencies | 539 small, medium and large organizations[154] (margin of error is +/- 3.6% at the 90% confidence level) | Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software | 2022 |
| 24% of maintainers have a defined dependency management process | Dependencies | 280 survey respondents[155] | Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report | 2023 |

[152] Context from the report: “Does that mean JavaScript is inherently more complex than .Net (49 dependencies), Go (56 dependencies), or Java (40 dependencies)? Not necessarily. In the case of JavaScript, each dependency often has a single purpose and small scope, rather than a library that fulfills multiple purposes with a large scope. Neither approach is more or less secure than the other, but knowing which dependencies you rely on (and how trustworthy they are) is an important part of vulnerability management”, Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software

[153] Further context from the report: “The survey sample was distributed by organization size as follows: small organizations (44%, 1-499 employees), medium organizations (20%, 500-4,000 employees), large organizations (35%, 5,000+ employees), and 1% don’t know or are not sure”, Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software

[154] Further context from the report: “The survey sample was distributed by organization size as follows: small organizations (44%, 1-499 employees), medium organizations (20%, 500-4,000 employees), large organizations (35%, 5,000+ employees), and 1% don’t know or are not sure”, Linux Foundation Research Team (2022): Addressing Cybersecurity Challenges in Open Source Software

[155] “Participants were contacted via Tidelift’s email lists and social media in November and December 2022”. Data is based on “339 respondents who a) maintain at least one open source project and b) completed a majority of the questions”, Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report

| Metric | Category | Scope | Source | Year |
|---|---|---|---|---|
| 40% of the most frequently used OSS packages had a release in the past two years as of March 2023 | Maintenance | First 10% of 6,592,414 packages[156] in the Ecosyste.ms dataset | Ecosyste.ms (2023): Packages | 2023 |
| 91% of OSS projects had no development activity in the last two years[157] | Maintenance | Black Duck Audit of 1,481 codebases[158] | Synopsys (2023): Open Source Security And Risk Analysis Report | 2023 |
| 40% of the most frequently used OSS packages had 5 or fewer maintainers | Maintenance | First 10% of 6,592,414 packages[159] in the Ecosyste.ms dataset | Ecosyste.ms (2023): Packages | 2023 |
| 44% are solo maintainers | Maintenance | 326 survey respondents[160] | Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report | 2023 |
| Contributors spent only 2.27% of their time on security-related efforts | Maintenance | Between 603 and 1.196 survey respondents[161] | Frank Nagle, David A. Wheeler, Hila Lifshitz-Assaf, Haylee Ham and Jennifer L. Hoffman (2020): Report on the 2020 FOSS Contributor Survey | 2020 |

[156] Excludes removed packages. Rated by average ranking, which is a combination score made up of relative downloads, dependent packages, dependent repos, stars and forks for each ecosystem.

[157] Further analysis from the report: "This probably means that the project is no longer being maintained, especially in the case of smaller projects", Synopsys (2023): Open Source Security And Risk Analysis Report

[158] Before opt-out, the audit included 1,703 codebases, of which 96% contained open source, Synopsys (2023): Open Source Security And Risk Analysis Report

[159] Excludes removed packages. Rated by average ranking, which is a combination score made up of relative downloads, dependent packages, dependent repos, stars and forks for each ecosystem. Excluded were ecosystems where the API does not provide data on the number of maintainers.

[160] "Participants were contacted via Tidelift's email lists and social media in November and December 2022". Data is based on "339 respondents who a) maintain at least one open source project and b) completed a majority of the questions", Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report

[161] Additional context from the report: "To capture a cross-section of the FOSS community, the research team distributed the survey to contributors to the most widely used open source projects (as determined by the previous "CII Census II Preliminary Report — Vulnerabilities in the Core.") and also invited the wider FOSS contributor community through an open invitation. The response distribution was usually similar between these two groups, though there were exceptions (e.g., different programming languages' prominence did vary). A total of 1,196 respondents filled out the demographic section and at least one question about current FOSS contributions, of whom 603 went through the entire survey", Frank Nagle, David A. Wheeler, Hila Lifshitz-Assaf, Haylee Ham and Jennifer L. Hoffman (2020): Report on the 2020 FOSS Contributor Survey

| Metric | Category | Scope | Source | Year |
|---|---|---|---|---|
| 52% of maintainers “are not aware of prominent software security standards” | Maintenance | 292 survey respondents[162] | Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report | 2023 |
| 58% of maintainers that are aware of industry security standards are either unsure or do not plan to align with these standards | Maintenance | 140 survey respondents[163] | Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report | 2023 |

[162] “Participants were contacted via Tidelift’s email lists and social media in November and December 2022”. Data is based on “339 respondents who a) maintain at least one open source project and b) completed a majority of the questions”, Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report

[163] “Participants were contacted via Tidelift’s email lists and social media in November and December 2022”. Data is based on “339 respondents who a) maintain at least one open source project and b) completed a majority of the questions”, Tidelift (2023): The 2023 Tidelift State Of The Open Source Maintainer Report

## B. Policy Interventions

| Policy Intervention | When |
|---|---|
| **Providing support to the OSS ecosystem:** | |
| • Supporting OSS security-relevant initiatives, infrastructure and tools | General |
| • Supporting OSS security research | General |
| • Providing threat intelligence | Continuous Integration and Delivery |
| • Supporting information-sharing projects, such as SBOM, CVE, VEX and CSAF | Post-Deployment |
| • Supporting adopt-a-package initiatives | End-of-Life |
| • Assessing end-of-life metrics | End-of-Life |
| **Cooperating with OSS communities:** | |
| • Engaging with OSS ecosystem | General |
| • Advocating for OSS communities | General |
| • Convening relevant stakeholders | General |
| • Serving as the point of contact for OSS project communities abandoning their projects | End-of-Life |
| **Setting the agenda of legal and policy changes:** | |
| • Adapting computer crime laws | Post-Deployment |
| • Providing a credible framework for a coordinated vulnerability disclosure process | Post-Deployment |
| • Establishing tax credits for OSS development | Post-Deployment |
| **Implementation of soft-touch interventions:** | |
| • Promoting OSS security interest in standardization working groups | Development |
| • Harmonizing existing development concepts | Development |
| • Nudging the security posture of providers of tools and infrastructure | Continuous Integration and Delivery |
| • Naming and shaming for not reporting bugs upstream | Post-Deployment |
| • Nudging developers to reshare improved code | Post-Deployment |

| Policy Intervention | When |
|---|---|
| **Taking concrete operational action:** | |
| • Providing software repositories of vetted versions of OSS that are used by government agencies | General |
| • Providing infrastructure for continuous integration and delivery | Continuous Integration and Delivery |
| • Sharing tools for continuous integration and delivery | Continuous Integration and Delivery |
| • Facilitating vulnerability reporting | Post-Deployment |
| • Identifying and mapping “no longer maintained” definitions | End-of-Life |
| • Alerting downstream users about end-of-life dependencies | End-of-Life |
| • Commissioning of patches, secure forks and rewrites | End-of-Life |
| **Funding of tools, services and infrastructure:** | |
| • Funding developer security tools and safer programming languages | Development |
| • Funding code-level security audits | Development |
| • Providing incentives to find bugs | Post-Deployment |
| • Funding tools and infrastructure | Continuous Integration and Delivery |
| • Providing a patch reward program | Post-Deployment |
| • Setting up a dedicated troubleshooting fund | End-of-Life |
| **Providing information and resources:** | General |
| • Providing resources for secure software development | Development |
| • Vetting and providing existing security-related resources, including security advisories, about tooling and infrastructure | Continuous Integration and Delivery |
| • Providing guidelines for software recycling and responsible sunsetting of projects | End-of-Life |

| Policy Intervention | When |
|---|---|
| **Improving education and training:** | |
| • Offering fellowships for securing software development | Development |
| • Improving education, for example, about secure software development practices, including corresponding guidelines | Development |
| • Supporting curricula development (and teaching) of secure software development | Development |
| **Supporting the government:** | |
| • Taking stock of government inventory of all OSS | General |
| • Assessing OSS projects that are critical for the government | Post-Deployment |
| • Advising legislative and executive branches | General |

## About Stiftung Neue Verantwortung

Stiftung Neue Verantwortung (SNV) is a non-profit think tank at the intersection of technology and society. At SNV's core is a methodology of collaborative development of policy proposals and analyses. SNV experts do not work alone – they develop and test ideas together with representatives from politics and public administration, technology companies, civil society and academia. Our experts work independently of interest groups and political parties. We guarantee our independence through diversified financing, comprised of contributions from different foundations, state and corporate actors.

## About Transatlantic Cyber Forum

To further policy research in the area of international cybersecurity and provide concrete recommendations, the Stiftung Neue Verantwortung (SNV) established The Transatlantic Cyber Forum (TCF) in January 2017. TCF is an intersectoral network and currently consists of more than 150 practitioners and researchers from civil society, academia and private sector working in various areas of transatlantic cybersecurity policy.

## About the Author

**Dr. Sven Herpig** is Director for Cybersecurity Policy and Resilience. He analyses the roles of government in vulnerability management, law enforcement hacking, responses to cyber operations, securing machine learning, and fostering open source security.

**Contact the author**

Dr. Sven Herpig
Director for Cybersecurity Policy and Resilience
sherpig@stiftung-nv.de
+49 (0) 30 81 45 03 78 91

# Imprint

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Alina Siebert