Atlantic Council CYBER STATECRAFT INITIATIVE DFRLab

AVOIDING THE SUCCESS TRAP: Toward Policy for Open-Source Software as Infrastructure

By Stewart Scott, Sara Ann Brackett, Trey Herr, and Maia Hamin *with the Open Source Policy Network*

CYBER STATECRAFT INITIATIVE

DFRLab

The Cyber Statecraft Initiative works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The author is solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

ISBN-13: 978-1-61977-263-2

February 2023

Design by: Donald Partyka and Anais Gonzalez

Cover image licensing language: CSI produced this report's cover image using in part OpenAI's DALL-E program, an AI image-generating application. Upon generating the draft image-prompt language, the authors reviewed, edited, and revised the language to their own liking and take ultimate responsibility for the content of this publication.

CYBER STATECRAFT
INITIATIVE

DFRLab

AVOIDING THE SUCCESS TRAP:

Toward Policy for Open-Source Software as Infrastructure

By Stewart Scott, Sara Ann Brackett, Trey Herr,
and Maia Hamin *with the Open Source Policy Network*

ACKNOWLEDGEMENTS

The authors owe a continuing debt of gratitude to the members of the Open Source Policy Network whose growing collaboration on open-source security and sustainability policy is an important part of this work. Major thanks to the Open Source as Infrastructure Working Group, including co-sponsor Open Forum Europe and its Executive Director Astor Nummelin Carlberg, whose insights shaped this report across 2022 and 2023. Thank you to Abhishek Arya, Jack Cable, Brian Fox, John Speed Meyers, Sarah Novotny, Jeff Wayman, and David Wheeler for their feedback on this and earlier drafts. Additional thanks to Kathy Butterfield, Estefania Casal Campos, and Abdolhamid Dalili for developing the report's graphics; to Nancy Messiah and Andrea Raitu for its web design; to Donald Partyka and Anais Gonzalez for graphic and document design; and to Jen Roberts for coordinating the project's many visual and design elements. This work is made possible with support from Craig Newmark Philanthropies, Schmidt Futures, the Open Source Security Foundation, and Omidyar Network.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

High-profile security incidents involving open-source software (OSS) have brought the ubiquity of OSS and the unique challenges its communities face to the attention of policymakers in the United States, EU, and beyond. For policymakers seeking to support the security and sustainability of OSS as a shared resource, this report builds on an important perspective on open-source software: **OSS as Infrastructure.** OSS is code published under a license that allows anyone to inspect, modify, and re-distribute the source code. This helps developers share and re-use solutions to common problems, creating such efficiencies that some estimate that 97 percent of software depends on OSS. OSS ranges from small components for illustrating graphs to entire operating systems. Contributors include individuals working in their free time, staff at large companies, foundations, and many others. The ecosystem is community-based, with many governance structures to manage contributions and maintenance.

This report compares OSS to three infrastructure systems—water management systems, capital markets, and networks of roads and bridges—and draws on existing policy vehicles from each to suggest policy that supports the sustainability and security of OSS as a communally beneficial resource.

Software borrows metaphors from **water systems**, including "upstream" and "downstream" relationships between packages and the end products that rely on them. Entities that use water from the ground or rivers do not assume its potability or perpetual availability—instead, they ensure the water is fit for their varying needs. OSS consumers have a responsibility to ensure the OSS they consume is well supported and secure, and the largest OSS users have the most responsibility for supporting ecosystem sustainability. OSS also bears similarity to **capital markets**, facing compounding, systemic risks, as chains of software dependencies can make a single OSS project a point of failure for many downstream systems. These risks intensify when there is little transparency or accurate reporting available to consumers—or regulators—to evaluate and mitigate risk. Finally, OSS has previously been compared to **roads and bridges**, and this bears out in the manner that insufficient investment in ongoing support creates risk over time. The collapse of a bridge—or the discovery of a vulnerability in a widely used OSS package—can focus attention and investment, but continuous, mundane maintenance to prevent such crises often falls by the wayside.

Taken together, these infrastructure systems—and the policy vehicles that support them—provide key principles for policymakers looking to support open-source software as infrastructure:

ENCOURAGING RESPONSIBLE OSS CONSUMPTION:

1. Get government to "walk the walk" of being a responsible OSS consumer by establishing one or more Open Source Program Offices in the federal government to help agencies manage their OSS strategy, policy, and relationships.

2. Develop an OSS Best Practices framework through NIST that incorporates risk assessments and contribution back to the OSS ecosystem. Industry and government could use the framework for self-assessment, and government could use it to help inform procurement evaluations.

3. Develop, through OSS-mature companies and nonprofits, a standard of best practices for contributing to OSS to bring in more OSS Good Samaritans from smaller organizations.

MITIGATING SYSTEMIC RISKS:

4. Create an Office of Digital Systemic Risk Management (ODSRM) within the Cybersecurity and Infrastructure Security Agency to identify systemic digital risks, including key widely used and at-risk OSS packages for targeted support.

PROVIDING RESOURCES WITH SECURITY AND SUSTAINABILITY IN MIND:

5. Establish a target-of-opportunity funding program to support maintenance and incident-response work for systemically important OSS projects.

6. Establish an OSS Trust Fund to provide sustainable and long-lasting investments in the security and maintenance of OSS code and the health and size of OSS maintainer communities.

7. Develop an adopt-a-package program through which companies provide resources to support ongoing maintenance and vulnerability mitigation for OSS packages they depend on. Such a program could encourage more small and non-IT-sector companies to take part.

1

INTRODUCTION

Open-source software (OSS) sits at the center of almost every digital technology moving the world since the early 1980s—laptops, cellphones, widespread internet connectivity, cloud computing, social media, automation, all the rainbow flavors of e-commerce, and even secure communications and anti-censorship tools. OSS, developed without exclusive ownership by globe-spanning communities, has enabled engineers, scientists, and entrepreneurs alike to build great, huge things and make momentous technological advances.

Much like the transcontinental rail systems of the nineteenth century and the intermodal shipping container system of the twentieth, OSS is an infrastructure that enables and shapes social, political, and economic activity across the world. Like the shipping container system and more than the highly visible railroad, OSS has long gone underrecognized outside of expert communities for the influence its code and developers have on the world.

That lack of recognition began changing only recently as OSS has come to the fore outside technology communities, with interest from philanthropic investors and grantmaking as well as congressional hearings after the December 2021 log4shell vulnerability.[1], [2] The challenge with much of this attention is its emphasis on there being something wrong with OSS, something "broken" or "inherently weaker" with the code that needs fixing. The mindset of putting out a fire in open source, without critically reevaluating the relationship between OSS developers and consumers as well as the need for material acknowledgment of the importance of open-source code, threatens the long-term sustainability and security of OSS.

Pathbreaking research from Nadia Eghbal[3] in 2016 helped present the public-policy challenge regarding OSS used to build essential technology systems. Not just an issue of shortfall in security, the OSS development model poses a basic problem of equity and value. OSS separates sale value, the amount a consumer is willing to pay for a free product, and use value, the amount this consumer gains by using it—an issue called out as early as 1997 by Eric Raymond.[4] There is

[1] "Critical Digital Infrastructure Research," Ford Foundation, accessed January 12, 2023, https://www.fordfoundation.org/campaigns/critical-digital-infrastructure-research/.

[2] Full Committee Hearing: "Responding to and Learning from the Log4Shell Vulnerability," US Senate Committee on Homeland Security & Governmental Affairs, February 8, 2022, https://www.hsgac.senate.gov/hearings/responding-to-and-learning-from-the-log4shell-vulnerability; Hearing: "Securing the Digital Commons: Open-Source Software Cybersecurity," House Committee on Science, Space, and Technology, May 11, 2022, https://science.house.gov/2022/5/joint.

[3] Nadia now goes by Nadia Asparouhova and more on her work can be found here https://nadia.xyz/

[4] Eric S. Raymond, *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (O'Reilly Media, Inc., 2001).

Figure 1. Survey responses

How much do you agree or disagree with the following statements? *A government role in supporting the open-source ecosystem is **necessary** for its long-term sustainability and success.*

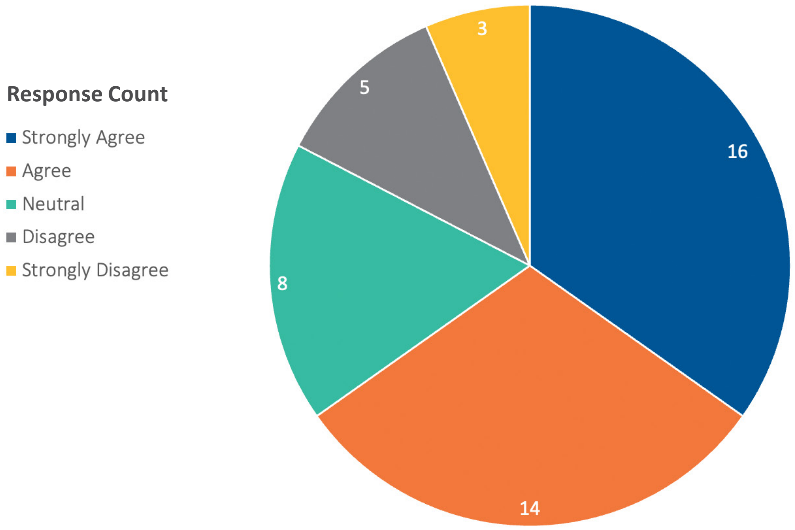
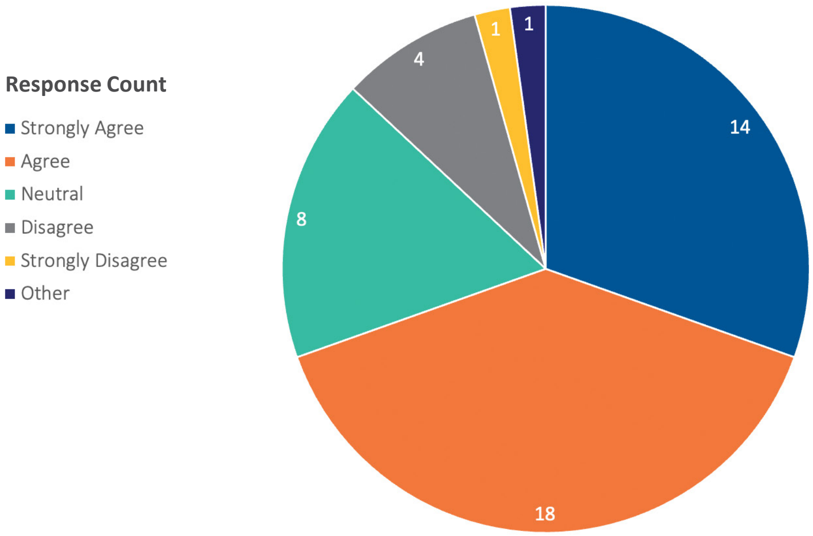


Figure 2. Survey responses

How much do you agree or disagree with the following statements? *Government support must include direct financial investment to ensure the open-source ecosystem's long-term sustainability and success.*



no clear market solution when conventional mechanisms to assign a value at sale and fractionally return that value to developers do not work. This kind of gap in a market opens a clear lane for public policy to do more than just support this infrastructure through the public purse. A survey conducted for this report,[5] discussed in more depth in the appendix, shows 65 percent of respondents agreed or strongly agreed on the necessity of a government role for the long-term health of the ecosystem. Moreover, 70 percent saw direct government funding as necessary to ensure this.

However, this is not to say that government is the only relevant player. Respondents indicated that, while they largely thought a government role in supporting the OSS ecosystem was requisite for its long-term health, they did not necessarily see it as the main party responsible for stepping up to the plate. This reflects a common thread of argument throughout this report: the criticality of OSS projects is determined not by their creators but by those using the package, and accordingly, responsibility for the ecosystem primarily rests in the hands of its largest beneficiaries—here, industry.

1.1 What Are We Doing Here?

This report builds on previous research by the Atlantic Council and others, as well as the collected insights of the Open-Source Policy Network,[6] to argue that public policy can address the systems' shortfalls by approaching OSS as infrastructure. Making policy to support and sustain OSS as infrastructure helps move viewing this code from a place of fear of security vulnerabilities to one that understands OSS as a critical component of an efficient software ecosystem, while still acknowledging the important role policy holds in improving security writ large.

When policy focuses only on terrible, potential outcomes, its ideas tend to reflect that bias toward fear, but this need not be the framing for OSS. Open source enables and solves much more than it imperils. Its security is as much a guarantor of continued value to users large and small, from individuals to national intelligence agencies, as it is a bulwark against malicious intent.

While OSS has come back to attention as an issue of national policy in the European Union (EU), and indeed become one for the first time in the United States in some ways as a product of fear and calamity, opportunities run much deeper. Infrastructure of such scale and magnitude is supported, reinforced, and amplified—not fixed in a brief whirlwind of activity—much like the consistent provisions of clean water, roads and bridges, and healthy capital markets. This report proposes clear models for sustained OSS support and offers guidance on how governments in the United States, European Union (EU), and nations across its member-state constituents can implement such models.

> *"Much like roads or bridges, which anyone can walk or drive on, open source code can be used by anyone… This type of code makes up the digital infrastructure of our society today."*
> *– Roads and Bridges: Unseen Labor*[7]

This report identifies key principles of OSS development and use. It relates them to other physical infrastructures for which there are mature policies and laws in an ensemble approach to combine nuance and tangible recommendations. The report points policymakers toward adaptable policies addressing more familiar forms of infrastructure that serve as case studies for government support of OSS. There are two reasons for this work.

First, as tangible as the infrastructure comparison is, OSS also has useful differences from physical infrastructure that offer opportunities for nuance. The open-source ecosystem is far more varied, complex, and dynamic than most physical infrastructure. Eghbal, for example, explains in detail the many differences between OSS and her chosen roads and bridges analogy.[8] Obscuring

[5] To the reader, as part of this report, the Atlantic Council and the Open-Source Policy Network distributed an anonymous survey to several OSS governance, policy, and security communities, including through the OpenSSF's general Slack channel and Open Forum Europe's email forum. The survey, open from November 20, 2022, through January 8, 2023, aimed to gather attitudes on OSS policy and security from OSS maintainers, developers, and stakeholder communities closer to the problem set than policymakers in Brussels or DC. Despite being open to over two thousand potential respondents, the survey only achieved a sample size of forty-six, limiting the insight into community priorities that it could provide. Nonetheless, there were some noteworthy trends in the responses, and the Atlantic Council and Open-Source Policy Network will continue to gather outside perspectives and sentiment trends in this manner.

[6] This project and the Open Source Policy Network are made possible with support from Craig Newmark Philanthropies, Schmidt Futures, the Open Source Security Foundation, and Omidyar Network.

[7] Nadia Eghbal, "Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure," *Ford Foundation*, June 14, 2016, https://www.fordfoundation.org/media/2976/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure.pdf.

[8] Eghbal, "Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure."

that nuance can lead policymakers to ignore obvious benefits—the substantial human communities involved in building and maintaining OSS, for example. OSS is, ultimately, the product of people with a variety of motivations, not the least of which are pure enthusiasm, curiosity, and a desire for community. Given the ecosystem's overwhelming variety, it is often more accurate to understand OSS as an expression of social interaction and group problem-solving. Rather than designed top-down, it is infrastructure that emerges.[9] OSS is fundamentally free speech in machine-readable form, not exquisite public works produced under a single engineering vision. Dynamic, interwoven groups of individuals produce, modify and maintain the code, rather than it being a commodity, product, or service *per se*, which carries significant ramifications for law and policy, as well as the infrastructure analogy.[10]

Second, as policymakers consider OSS in the larger context of significant cybersecurity policy in the United States, a set of guiding principles would help predict and model policies' impact on OSS. Common physical infrastructure shares similarities to OSS: both support critical functions, provide dependable services, offer subtle and often unseen service delivery, function through systems of decentralized control, and more. Government has long engaged in infrastructure policy, so drawing on those more familiar frameworks offers opportunity to hone engagement with, and support for, the OSS ecosystem.

To better capture the complexity of the OSS ecosystem, this report offers not one but three infrastructure analogies for OSS policy. They are water-management systems, capital markets in the financial services sector, and roads and bridges from Eghbal's report. The comparison between OSS and water-management systems invokes both systems' sprawling networks of producers, intermediaries, quality assurers, and varied use cases. It also highlights the relationship between the degrees of usage and responsibility to the overall sustainable functioning of the ecosystem and discusses policy models based on Nevada water law and federal regulations around funding and protecting volunteer clean-up efforts. The comparison to the financial sector focuses on the nature of risk and transparency in both domains, where a variety of modular, interconnected, and aggregated items (projects in OSS, assets in finance) create nodes of risk and leverage and where risk management relies on insight into the location and of function of underlying system components. The section looks at policy efforts to identify and manage systemic risk created in these networks of dependence. Last, the roads and bridges comparison builds on Eghbal's report, highlighting the importance of continual maintenance, funding, and tailored intervention across an interconnected network. It looks to the Highway Trust Fund (HTF) and adopt-a-highway programs for models of funding and support for key infrastructure.

> *"Open source software is part of the foundation of digital infrastructure that promotes a free and open internet"*
> *– S.4913, The Securing Open Source Software Act of 202211[12]*

For each analogy, the report addresses the prominent characteristics shared with the OSS ecosystem, explores the comparison in depth, and surfaces guiding policy principles before offering examples of relevant US and EU policies as potentially useful models for OSS. Following these analogies is a discussion of some existing government policies toward OSS and specific recommendations.

This report aims to develop tangible example policies for the United States and European Union to support OSS as infrastructure and point policymakers toward existing policy vehicles that government can readily modify and adopt to better support and engage with the OSS ecosystem. The report does not seek to make definitive statements about what open source is or is not through these analogies. Rather the goal is to capture a snapshot of its most essential features and most consequential participants. Any of the analogies can be extended far past usefulness, and policymakers should approach each keeping in mind the essential truth that, while all models are wrong, some (including, we believe, these) are useful, nonetheless. Before diving into the analogies though, this report looks to discuss the open-source ecosystem as it is, highlighting key principles and addressing common misconceptions.

[9] Julia Ferraioli, "Open Source and Social Systems," (blog), December 7, 2022, https://juliaferraioli.com/blog/2022/open-source-social-systems/.

[10] Alison Dame-Boyle, "EFF at 25: Remembering the Case That Established Code as Speech," Electronic Frontier Foundation, April 16, 2015, https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech.

[11] "Securing Open Source Software Act of 2022," S.4913, 117th Congress (2022), https://www.congress.gov/bill/117th-congress/senate-bill/4913.

[12] Eghbal, "Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure."

2

THE OPEN-SOURCE ECOSYSTEM

While the motives of software developers can vary from securing a paycheck to satisfying personal curiosity, most software itself ultimately strives to carry out a task or solve a problem. Open-source software (OSS) is an acknowledgment that many such problems are similar and repeatedly encountered by developers. OSS works by making one solution to a problem available to all to re-purpose and re-use, which likely results in a strong return on investment (ROI),[13] both financially and socially.[14] While there are several different legal approaches to defining and licensing what is "open source," the common OSS philosophy grants forward to users and consumers the rights to inspect, modify, and redistribute software—its source code is "open."[15] In this, OSS generally differs from closed-source or proprietary software by providing these additional rights.

The result is a vast network of overlapping communities principally involved with developing, maintaining, and integrating OSS. These communities range from volunteers to paid professionals, with participants who exist entirely outside the for-profit technology industry and myriad others who are full-time employees from the likes of Google, Microsoft, and Amazon.

While open source as a philosophy predates the internet—witness the chaotic ballet of licensing and development values that characterized the 1969 birth of Unix and its fractured gestation as one example[16]—the internet proved a tremendous accelerant to OSS development. Indeed, the emergence of online

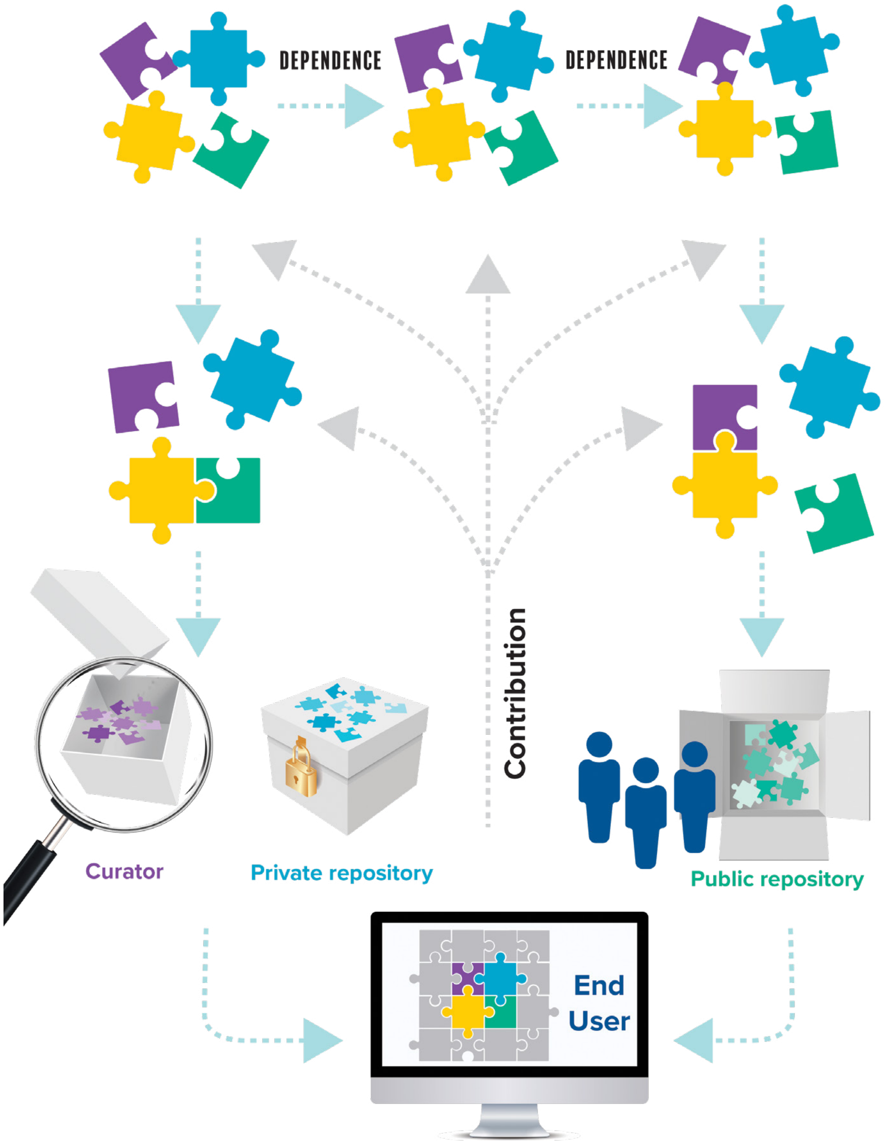
[13] Frank Nagle, "Government Technology Policy, Social Value, and National Competitiveness," Harvard Business School Strategy Unit Working Paper No. 19-103, March 3, 2019, https://doi.org/10.2139/ssrn.3355486.

[14] Karl Fogel and Cecilia Donnelly, "Open Data for Resilience Initiative and GeoNode: A Case Study on Institutional Investments in Open Source" (Washington, DC: World Bank Group, December 31, 2017), http://documents.worldbank.org/curated/en/713861563520709009/Open-Data-for-Resilience-Initiative-and-GeoNode-A-Case-Study-on-Institutional-Investments-in-Open-Source; Knut Blind et al., "Study about the Impact of Open Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy | Shaping Europe's Digital Future" (Brussels: European Commission, September 6, 2021), https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and; Brian Proffitt, "The ROI of Open Source," Red Hat Blog, August 26, 2020, https://www.redhat.com/en/blog/roi-open-source. To the reader, while the authors of this report are not aware of replication studies validating these findings, it is worth noting that the sheer ubiquity of OSS already in proprietary offerings indicates the widespread success of the model. Whether that is due to reduced development time, crowd-sourced innovation, or other factors is not clear, however.

[15] "The Open Source Definition," Open Source Initiative, accessed January 13, 2023, https://opensource.org/osd.

[16] Peter Salus, The Daemon, The Gnu, and the Penguin, (Reed Media Services, September 2008).

Figure 3. Dependencies and contributions



communities developing and maintaining open-source code helped meaningfully differentiate the internet from precursor telecommunications networks and gave tangible form to Licklider and Taylor's vision of creative communications among thinking machines. [17]

There are several key characteristics of the open-source ecosystem for policymakers to keep in mind. First among these is its sheer scale and variety. Though treating open source as a monolithic concept is a convenient abstraction—and for high-level policy, a necessary one at least up to a point—the real landscape is staggeringly diverse. There are communities built around specific programming languages, from commonly known Python to the deliberately esoteric Befunge.[18] Some communities center on specific projects like the Linux kernel, and others orbit downstream functions like encrypted communications tools or specialized statistical analysis packages. Some projects serve simple ends like correctly adding characters to the left of a string or number.[19]

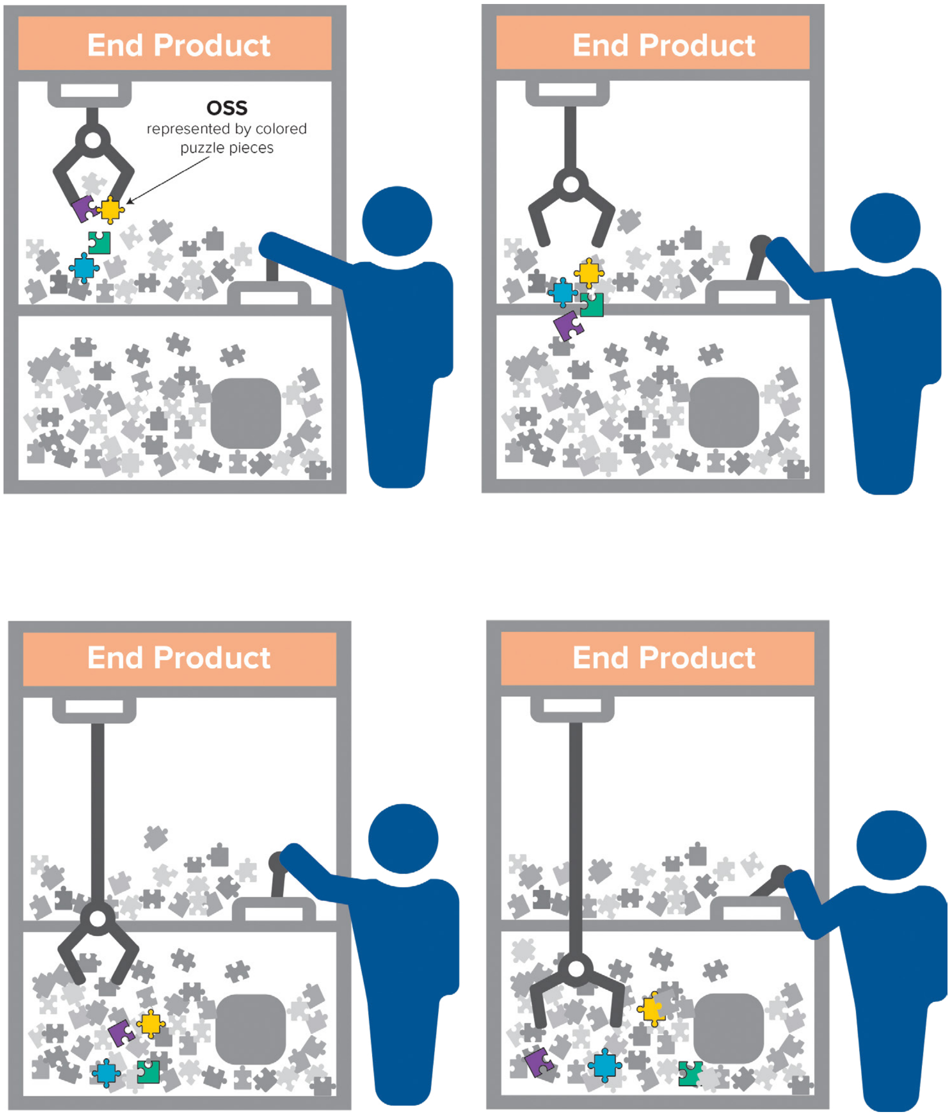
[17] Joseph Carl Robnett Licklider and Robert W. Taylor, "The Computer as a Communication Device," Science and Technology 76 (April 1968), 21–31.

[18] befunge, GitHub, accessed January 13, 2023, https://github.com/topics/befunge.

[19] Left-Pad, Node.js Package Manager (npm), accessed January 13, 2023, https://www.npmjs.com/package/left-pad.

Others provide word-processing programs[20] or even entire operating systems, such as Linux and its many distributions.[21] There are open cloud platforms such as OpenStack and open container orchestration systems like Kubernetes. There are also open-source code compilers, web servers, media players, and so on—some open source functions as standalone applications, some as deeply buried components for repurposing in different contexts. Some assembles programming languages into executable binaries, some builds software, some analyzes code for bugs, and so on.

Figure 4. Buried OSS relationships



[20] LibreOffice, accessed January 13, 2023, https://www.libreoffice.org/.

[21] "Linux Distribution Introduction and Overview," Linux Training Academy, accessed January 13, 2023, https://www.linuxtrainingacademy.com/linux-distribution-intro/.

The relationships between OSS projects and the larger software world are also complex and widely varying. A useful term here is "depth in stack," referring to how deeply buried within an overall product or application OSS and other components can be. The most straightforward use of OSS might be in user-facing applications—for example, instead of purchasing Microsoft Word, one might download and use LibreOffice, an open-source word processor that provides largely the same functions as Word.[22] A similar simple example of incorporating OSS into a project could include an academic researcher writing a data-analysis script in R, a commonly used statistics language. They might include the lines "install.packages(ggplot2)" and "library(ggplot2)" at the top of their script, giving them access to a variety of graphing tools and functions as they analyze a dataset.[23]

Other instances of OSS reliance run far deeper and are more challenging to map out. A user in the simple act of watching a show on Netflix relies on an immense variety of OSS, from the streaming platform's own open-sourced projects to the guts of the underlying Amazon Web Services (AWS) cloud instances,[24] which include server operating systems, container orchestrators, and innumerable component services. The log4shell incident highlighted just how deeply buried OSS dependence can be and, accordingly, how challenging the task of identifying dependence is. One report found that 60 percent of log4j uses were indirectly rather than directly implemented, challenging remediation efforts.[25] One study by Qualys found that as of March 2022, some 30 percent of log4j instances remained unpatched.[26] This pattern holds across the ecosystem, where dependence is rarely obvious and easily identified when OSS components lie buried beneath indirect relationships and obscure references.

While all the above mainly considers the open-source ecosystem through the lens of the code, keeping its human basis in mind is critical. Members of the open-source ecosystem can wear many hats, from running a hobby project to integrating OSS into industry products in their day job, often moving between different communities, contexts, and ecosystems. Even the common roles for a given open-source project are fluid—a developer might open-source one of their projects and act as its maintainer while they continue to contribute.[27] Down the line though, either from lost interest in the project or not enough time to dedicate to its maintenance, a developer might call in a well-known contributor as a maintainer, either transferring the project over entirely or creating a team of maintainers. Different communities rely on different governance models, from maintainer-controls-all to elected positions for a project or select individuals relied upon for commit reviews. These OSS participants also distribute geographically, their contributions enabled by the foundational transparency of the ecosystem.

> *"It is helpful to frame open source as many different, interacting ecosystems. They evolve, respond to stimuli, compete, collaborate, have cultures, and follow norms. Actions that impact an open source ecosystem can have ripple effects beyond that ecosystem – and beyond the world of proprietary technology or even technology altogether."*[28]

[22] LibreOffice.

[23] ggplot2, accessed January 13, 2023, https://ggplot2.tidyverse.org/.

[24] Andrew Spyker and Ruslan Meshenberg, "Evolution of Open Source at Netflix," Netflix Technology Blog, October 28, 2015, https://netflixtechblog.com/evolution-of-open-source-at-netflix-d05c1c788429.

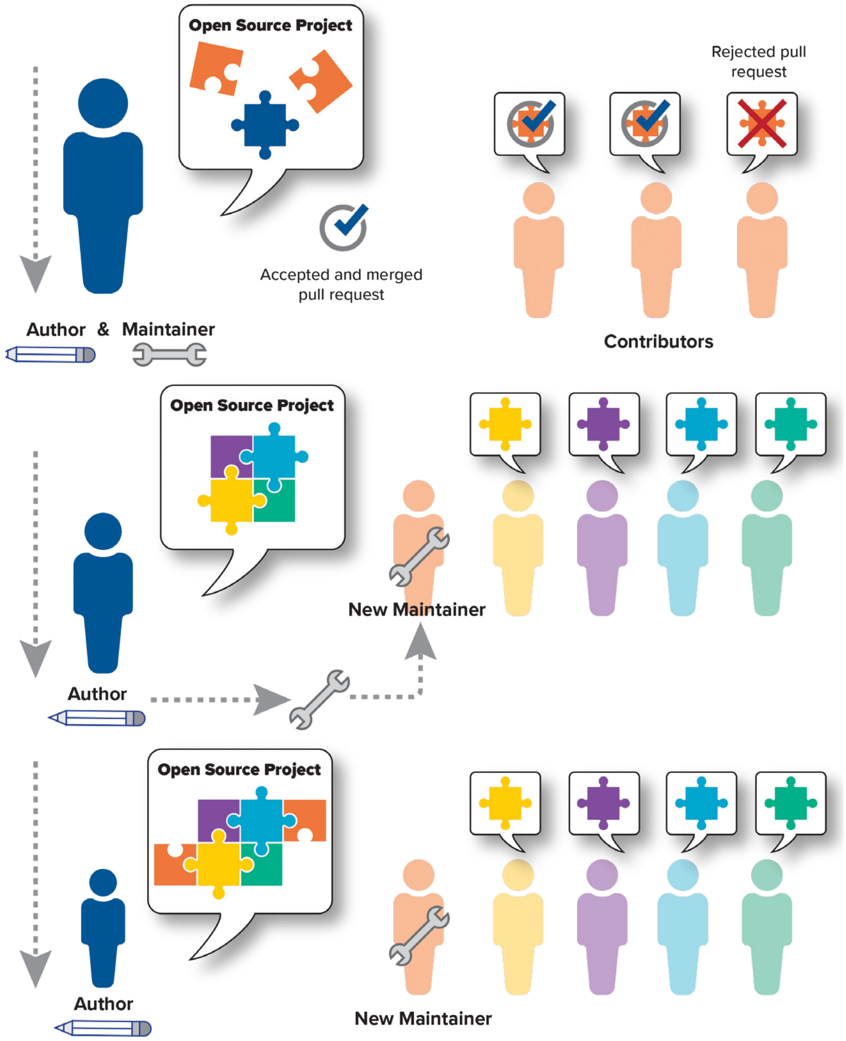
[25] Liran Tai, "The Log4j Vulnerability and Its Impact on Software Supply Chain Security," Snyk, December 13, 2021, https://snyk.io/blog/log4j-vulnerability-software-supply-chain-security-log4shell/.

[26] Mehul Revankar, "New Study Reveals 30% of Log4Shell Instances Remain Vulnerable," Qualys Security Blog, March 18, 2022, https://blog.qualys.com/qualys-insights/2022/03/18/qualys-study-reveals-how-enterprises-responded-to-log4shell.

[27] To the reader, using the term "open-source" as a verb means to make the source code available to all, often on a code hosting platform, with GitHub being one of the most commonly used repository hosts.

[28] Ferraioli, "Open Source and Social Systems."

Figure 5. Maintainer and contributor relationship



While OSS directly invokes "the code" and its developers, there also exists a staggering array of intermediary entities supporting and shaping the software side of things. Code hosts (sometimes called "forges") store the actual code in either public or private repositories—for example, Microsoft's GitHub, though there are myriad other hosts.[29] Registries or indices, like Node Package Manager (npm) and the Python Package Index (PyPI), record official versioning and documentation for some packages, though their code might reside on a code host like GitHub or be mirrored there. Package managers like Python's Preferred Installer Program (PIP) are the tools that, starting with a user command, retrieve the necessary code from a repository. At the more human level, nonprofits—many of them business leagues, like the Linux Foundation or Open Source Collective[30]—provide financial support for programs, and others, like the Open Source Initiative, manage licensing definitions.[31] Some

[29] Milo Z. Trujillo, Laurent Hébert-Dufresne, and James Bagrow, "The Penumbra of Open Source: Projects Outside of Centralized Platforms Are Longer Maintained, More Academic and More Collaborative," EPJ Data Science 11, no. 1 (May 21, 2022): 1–19, https://doi.org/10.1140/epjds/s13688-022-00345-7.

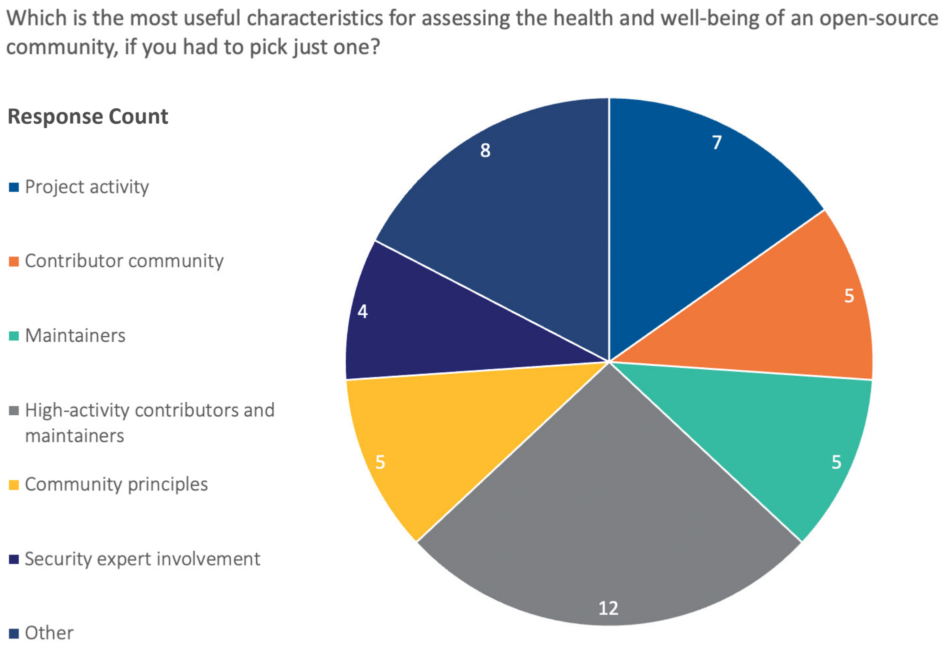
[30] To the reader, these fall under the 501(c)(6) classification. Their main difference from a 501(c)(3) nonprofit is that where (c)(3) organizations must serve the public, (c)(6) organizations must their members. For more detail, see Internal Revenue Services, "Business Leagues," irs.gov, accessed January 12, 2023, https://www.irs.gov/charities-non-profits/other-non-profits/business-leagues.

[31] "Licenses & Standards," Open Source Initiative, accessed January 13, 2023, https://opensource.org/licenses.

groups might provide security tooling or developer support to specific projects—for instance, the Alpha-Omega project assists maintainers of critical open-source projects.[32]

All this is to say that the open-source ecosystem is complex. With that complexity comes disagreement, and assuming consensus among the ecosystem's participants is an oversimplification similar to presuming that the code is uniform and governance structures straightforward. Some of the key debates among OSS communities will have direct policy implications. Some maintainers worry about where their projects might end up used,[33] some are wary of corporate involvement in the space shaping project direction and governance,[34] and others see OSS as a path toward a digital right to repair.[35] The survey conducted for this report reflects this diversity in priorities well. What respondents considered the greatest source of risk for the OSS ecosystem ranged widely, including technical concerns about memory-safe languages, practices for transferring project ownership, government overregulation, misunderstood or disregarded OSS community values, unknown and deeply intertwined dependencies, the insufficiency of economic models, maintainer burnout and overburdening, and even maintainer sabotage. Similarly, there was little consensus on what metric best captured the overall health and well-being of an open-source project community, with the number of active contributors and maintainers being the only standout answer, and not by a wide margin. As a policy report first and foremost, many of these discussions are out of scope here, but they are nonetheless important to policymakers.[36]

Figure 6. Survey responses



[32] Alpha-Omega, Open Source Security Foundation, accessed January 13, 2023, https://openssf.org/community/alpha-omega/.

[33] David Gray Widder, "Can You Stop Your Open-Source Project from Being Used for Evil?," Overflow, August 8, 2022, https://stackoverflow.blog/2022/08/08/can-you-stop-your-open-source-project-from-being-used-for-evil/.

[34] John Sullivan, "Thinking Clearly about Corporations," Free Software Foundation, June 24, 2021, https://www.fsf.org/bulletin/2021/spring/thinking-clearly-about-corporations.

[35] Sam Williams, Free as in Freedom: Richard Stallman's Crusade for Free Software (O'Reilly Media, Inc., 2002), https://www.oreilly.com/library/view/free-as-in/9781449323332/.

[36] To the reader, footnote entries offer further readings on the larger ecosystem and some of its defining debates.

3

OSS AS INFRASTRUCTURE: THREE ANALOGIES

3.1 Defining Infrastructure

Infrastructure rests as the "…vitally important, if not absolutely essential…" component that enables people to thrive, to create, and to build.[37] Infrastructure is the underlying plumbing under great ideas. Some definitions lean toward the tangible, roads, bridges, software code, and computer networks. Others emphasize the economic categorization—infrastructure as a public good. However, not all kinds of infrastructure fulfill the strict economic definition of being both non-excludable and non-rivalrous entailed.

Even physical infrastructure is not so easily defined and sees a significant amount of "know it when you see it" classification—for instance, the Cybersecurity and Infrastructure Security Agency (CISA) lists sixteen critical infrastructure sectors, with the selection criteria emphasizing *critical* far more than *infrastructure*.[38] OSS is present within traditional critical sectors, serving as infrastructure in a very literal sense.[39] For this report's purposes of guiding policy, significant similarity between OSS and infrastructure is sufficient, and there is plenty to find.

First, OSS handles many of the digital world's unseen, "nitty-gritty" tasks upon which the larger digital ecosystem relies. Take, for instance, any of the following: OpenSSL, OpenStack, Kubernetes, the GNU Compiler Collection, BIRD, and Linux running on most large internet servers—all these functions are core to

[37] To the reader, Dr. Tracy Miller defines infrastructure as "facilities, structure, equipment, or similar physical assets…vitally important, if not absolutely essential, to people having the capabilities to thrive…in ways critical to their own well-being and that of their society, and the material and other conditions which enable them to." See: Tracy Miller, "Infrastructure: How to Define It and Why the Definition Matters," Mercatus Center, July 12, 2021, https://www.mercatus.org/research/policy-briefs/infrastructure-how-define-it-and-why-definition-matters.

[38] "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency, accessed January 12, 2023, https://www.cisa.gov/critical-infrastructure-sectors.

[39] David Wheeler, "Securing Open Source Software Is Securing Critical Infrastructure," Open Source Security Foundation (blog), October 11, 2022, https://openssf.org/blog/2022/10/11/securing-open-source-software-is-securing-critical-infrastructure/.

digital services and largely hidden from end users.[40] Another striking example is cURL, which stands for client Uniform Resource Locator (URL) and pronounced curl informally.[41] It is a command line tool and library to handle data transfers, residing within internet servers, gaming consoles, automobiles, operating systems, smartphones, and more.[42] Consumers rely on digital systems for communications, financial transactions, transportation, healthcare, and other vital services—and many of those digital systems rely on OSS.

Second, beyond this necessary but less visible support, both OSS and physical infrastructure scale massively beyond their immediate surroundings, enabling huge swathes of the economy, end-user products, and more. One frequently cited report from Synopsys found that 78 percent of code in surveyed codebases was open source, while 97 percent of codebases contained at least some OSS.[43] Buried in the settings of every iPhone (Settings > General > Legal & Regulatory > Legal Notices) is a four-thousand-line-long, barely navigable list of all the licenses declared by the phone, many of which concern the open-source components it relies on—including, in iconic OSS style, "'THE BEER-WARE LICENCE' (Revision 42)…As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return."[44]

Third, much of what physical infrastructure accomplishes happens out of immediate public view and is easily taken for granted, despite its centrality to a smoothly functioning society. Rarely does the end user think of complex tangles of transmission lines, transformer hubs, and powerplants when flicking on a light switch—except when the lights stay dark. Similarly, most end users are unaware of the role that OSS plays in the digital systems that underpin their daily lives. Likewise, that dependence remains underappreciated until disruption of the end service.

Fourth and finally, the variety of forms of "ownership" or stewardship of OSS mirror the complex web of federal, state, local, and private ownership of physical infrastructure. In physical infrastructure, some sectors see almost complete federal ownership, some feature neat division among state or local governments and industry, and others rely on the many distribution patterns in between these.[45] For OSS, some projects are individually maintained, others housed in nonprofits or funded by foundations or trade organizations, some with support from large information technology (IT) vendors, or even maintained and curated by for-profit companies, and more. Some technology companies develop software projects in-house before "open sourcing" them out into the world. The variety of governance models in both domains requires careful, targeted, and flexible policy.

Industry players have repeatedly emphasized that OSS insecurity largely reflects the challenges of securing any kind of software—vulnerabilities are inevitable and agnostic to licensing.[46] The US government, meanwhile, has focused its most prominent efforts on OSS through a security lens—the first bill in Congress addressing OSS as an ecosystem, S.4913, is the Securing Open Source Software Act of 2022, and congressional testimony,

[40] Steven Vaughan-Nichols, "Can the Internet Exist without Linux?," ZDNet, October 15, 2015, https://www.zdnet.com/home-and-office/networking/can-the-internet-exist-without-linux/; "Cloud Infrastructure for Virtual Machines, Bare Metal, and Containers," OpenStack, accessed January 13, 2023, https://www.openstack.org/; "Welcome to OpenSSL!" Open Secure Sockets Layer (OpenSSL) Project, accessed January 13, 2023, https://www.openssl.org/; Nate Matherson, "26 Kubernetes Statistics to Reference," ContainIQ, July 3, 2022, https://www.containiq.com/post/kubernetes-statistics; "The BIRD Internet Routing Daemon Project," BIRD, accessed January 12, 2023, https://bird.network.cz/.

[41] Curl, accessed January 13, 2023, https://curl.se/.

[42] Daniel Stenberg, "The World's Biggest Curl Installations," (blog), September 17, 2018, https://daniel.haxx.se/blog/2018/09/17/the-worlds-biggest-curl-installations/.

[43] "Open Source Security and Risk Analysis Report," (Mountain View, California: Synopsys Inc., 2022), https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2022.pdf.

[44] To the reader, authors tip their hats to the researchers at Chainguard for pointing this out.

[45] Jennifer Bennett et al., "Measuring Infrastructure in the Bureau of Economic Analysis National Economic Accounts" (Suitland, MD: Bureau of Economic Analysis, December 1, 220AD).

[46] "The United States Securing Open Source Software Act: What You Need to Know," Open Source Security Foundation (blog), September 27, 2022, https://openssf.org/blog/2022/09/27/the-united-states-securing-open-source-software-act-what-you-need-to-know/.

and other spurts of government attention tend to react to security incidents like log4shell and Heartbleed. In one dataset of OSS government policies, security and modernization were the two most popular stated purposes for US policies related to OSS, with security holding the majority in the proposed legislation.[47]

This security focus does not and should not imply that OSS is in any way less secure than proprietary code. The two are not so easily distinguished, and the ability of anyone to review OSS for vulnerabilities should, at least in theory, make it more securable, if not secure, than obscured proprietary software. Rather, the fact that OSS underpins so much software and modern infrastructure means that its security, which is subject to some different incentives and forces than proprietary offerings, is of notable importance. This is like how CISA focuses on securing infrastructure not because it is innately insecure, but because it is critically important to the national interest. OSS is already as commonplace, structurally critical, and hidden from end users as rebar inside the reinforced concrete of a bridge span. It is equally critical, mundane, and—in some circles—unappreciated as the water treatment plants which ensure healthy drinking water or the catenary wires above an electric train. Where that criticality exceeds the ability of other policy levers to create change, a security lens helps prioritize action and investment, especially when shaping industry behavior.

3.2 Three Analogies

Treating OSS as infrastructure also invites other forms of engagement without exclusivity. While some governments might focus on supporting the security of OSS insofar as it is infrastructure, others can focus on investing in it for the holistic benefits to society or for the influence it might provide their countries in shaping the future social impact of important technologies. Infrastructure corresponds to investment and provides a ready framework for international cooperation. An infrastructure framing allows stakeholders to hold independent priorities under common, unifying principles.

Different characteristics of the OSS ecosystem evoke different kinds of infrastructure. This section describes the report's ensemble model: three analogies each mapping from principles shared by open source and a form of infrastructure to offer policy takeaways for the open-source ecosystem. Each analogy uses the language of tangible infrastructure alongside real-world policies that invest in, and support, this infrastructure. The table below summarizes these shared principles, infrastructure comparisons, and policy takeaways, in addition to the broader commonalities between physical infrastructure and OSS noted so far.

None of these analogies is complete on its own. Taken together, they present a practical view of much of what makes OSS work and work well at that. The takeaways intend to steer policymakers toward practical, considerate models for policy action shaped by lessons previously learned and concepts properly ordered.

This section also provides several direct models for the beginnings of government support for OSS—these are not prescriptive policy recommendations but rather tangible examples of how the investment of funds and other resources can help better support OSS. These models highlight effective parallels to OSS policy challenges either through the problems and questions they address, the intervention strategies they offer, the systems dynamics they navigate, or some combination.

[47] "Government Open Source Policies," *Center for Strategic and International Studies*, August 2022, https://www.csis.org/programs/strategic-technologies-program/government-open-source-software-policies.

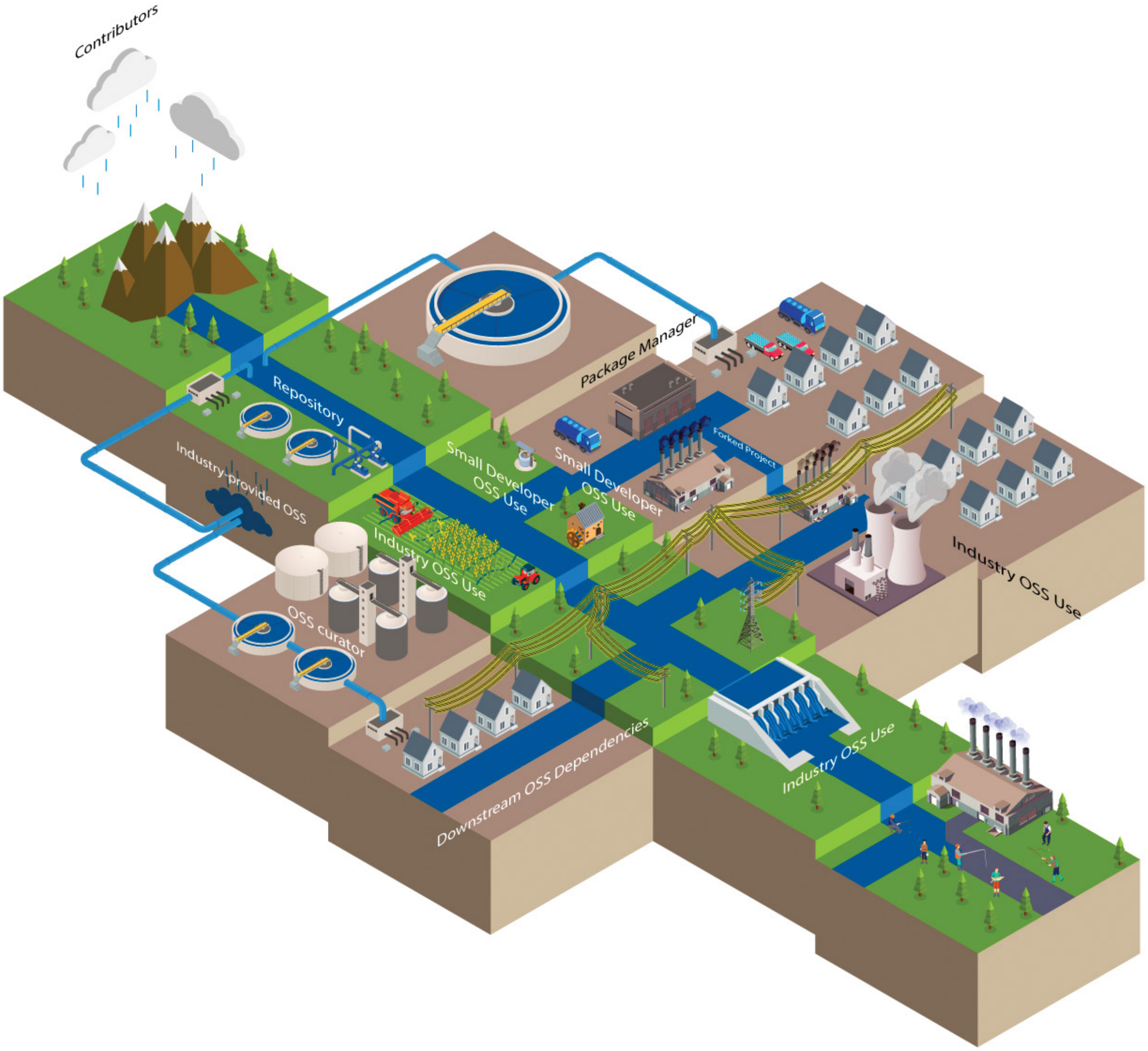
Figure 7. Table of shared principles of infrastructure and open source

	Similarity	Takeaway Principles	Parallel Policies
Water Management 	• Immense variety of interlinking, valid use cases from a common, underlying resource. • Relationship between use, source, and overall ecosystem health.	• Importance is determined by the act of use, not creation. • The source makes no representation about safety; consuming and consuming securely are different acts. • Health and safety are determined by collective behavior, rarely one point of action.	• Nevada Senate Bills 47 and 74 • Federal Good Samaritan Protections • EU Water and Waste Framework Directives
Capital Markets 	• Leverage and dependency create systemic risk. • System provides an enabling input to vast swathes of social and economic activity.	• Transparency and visibility enable risk management. • Targeted support is more effective than blanket policies.	• Financial Stability Oversight Council (FSOC) • European Securities and Markets Authority
Roads and Bridges 	• Correlation between criticality or usage and need for maintenance. • Investment by the few, use by the many. Few transactions exist on which to 'tax' use to benefit creation and maintenance. • Agnostic to end destination or outcome.	• Centralized funding works best through entities with local expertise. • Unglamorous maintenance beats recovering from catastrophe. • Criticality stems from frequency of use as well as lack of alternatives.	• Highway Trust Fund (HTF) • Adopt-a-Highway Programs • Connecting Europe Facility (CEF) and Cohesion Fund (CF)

3.2.1 Water Management Systems

Water management and distribution systems share two crucial characteristics with the open-source ecosystem. Most visible are both systems' continuous, directional relationships. Software development speak already roots itself in hydrologic nomenclature. The "upstream" and "downstream" relationships borrow from literal descriptions of rivers to describe how choices along supply chains impact different participants. Often, though not exclusively, these relationships explain the trickle-down impact of upstream incidents—for instance, the downstream users exposed to the recent log4shell vulnerability, or when the deletion of a little-known package called left-pad briefly broke websites across the world.[48] For water management and distribution systems, an upstream issue with a dam might impact water levels downriver, or changes in weather patterns might disrupt aquifer replenishment, causing shortages for downstream users, whether industrial, agricultural, or otherwise.

Figure 8. Water management and open source



[48] Sean Gallagher, "Rage-Quit: Coder Unpublished 17 Lines of JavaScript and 'Broke the Internet,'" Ars Technica, March 25, 2016, https://arstechnica.com/information-technology/2016/03/rage-quit-coder-unpublished-17-lines-of-javascript-and-broke-the-internet/.

This straightforward language about chains of dependency and shared exposure also describes another similarity between water infrastructure and OSS: the obligation of its users to contribute to the sustainability of the larger ecosystem, from statewide apportionment of the Colorado river to agricultural collectives deciding on the usage of local aquifers. For both water and OSS, a relatively small subset of users relies more heavily on shared resources than others. Hydroelectric facilities and large farms can use more water in an hour than an average household does in a year.[49] Likewise, massive IT vendors ship widely used products incorporating numerous open-source projects, while a researcher might rely on only a handful of packages aiding in statistical analysis.

While the policy solutions to protect the sustainability of water and the security of OSS do not map perfectly—a hard quota on industry use of OSS makes little sense. For example, as OSS is a non-rivalrous resource, the general ethos is critical: the largest users carry the largest obligations (and capacity) to contribute back to the sustainability of the ecosystem. Just like growing populations and a changing climate mean that water consumers and policymakers need to invest in conservation and sustainability,[50] the growth and increasing criticality of the OSS ecosystem means that OSS consumers and policymakers must understand that the availability and innate usability of the underlying code cannot be guaranteed without support. Few expect that water taken directly from a stream or pond be immediately potable. Neither should consumers assume the security and independent governance capacity for OSS projects as pulled into products without some level of security assurance and code review. Again, not because OSS is any less secure than proprietary offerings, but because it is all too likely that projects were developed without specific consumer usage in mind, and therefore, consumers should not expect them to cater to their exact management needs. An overriding principle of open-source licenses is that this code is delivered “as is.”

Water infrastructure also highlights the immense varieties in use, governance, and creation in the open-source ecosystem. Just as water fuels textile production, energy generation, and individual consumption alike, OSS has a wide variety of use cases, including hobbyist tinkering, academic research, internet functionality, and business- and product-critical operations. Open source and water management systems also feature large networks of intermediaries between easily conceptualized endpoints (e.g., developer and end user, mountain spring and sink faucet). Water does not just flow, uninterrupted, from a stream or spring into a residential tap, but instead twists through a series of reservoirs, canals, treatment facilities, and plumbing. In the same way, much OSS finds itself incorporated into software projects, those projects into others, and over again through other projects maintainers, repository hosts like GitHub, private mirrors within companies, curators like Red Hat, auditors like the Open Source Technology Improvement Fund (OSTIF), transitive dependencies of other projects, and more before ever reaching a user.

Many OSS stakeholders worry that government investment and support will bring onerous obligations and regulations for developers,[51] whether in the form of liability or excessive documentation, that risk dissuading developers from providing open-source systems. Water management systems provide a clear parallel example of an alternate approach. In the same way that companies and individuals do not assume the purity of water in unknown streams or springs, neither should they assume that volunteer developers, often uncompensated for their work, have provided perfectly secure code and will bear total responsibility for repairs and upkeep. Most open-source licensing bears out this relationship, including something to the effect of the Apache 2.0 license’s phrasing: the “licensor provides the work (and each contributor provides its contributions) on an ‘as is’ basis, without warranties or conditions of any kind.”[52] OSS users, especially the largest and best-resourced, should bear more of the responsibility for supporting the security, and appropriate selection, of open-source software, rather than using blithely and thereby trusting warranties never promised. Among more mature OSS consumers—particularly large IT vendors—this relationship is well realized, with vendors like Microsoft, Google, and others investing significant funds and developer time into the

[49] “How We Use Water,” Overviews and Factsheets, US Environmental Protection Agency, accessed January 13, 2023, https://www.epa.gov/watersense/how-we-use-water.

[50] Rachel Estabrook and Michael Elizabeth Sakas, “The Colorado River Is Drying up — but Basin States Have ‘No Plan’ on How to Cut Water Use,” Colorado Public Radio, September 17, 2022, https://www.cpr.org/2022/09/17/colorado-river-drought-basin-states-water-restrictions/.

[51] Ashwin Ramaswami, “Securing Open Source Software Act of 2022,” Sustain Open Source Forum, October 3, 2022, https://discourse.sustainoss.org/t/securing-open-source-software-act-of-2022/1098.

[52] “Apache License, Version 2.0org,” Open Source Initiative, accessed January 13, 2023, https://opensource.org/licenses/Apache-2.0.

OSS ecosystem.[53] Governments can participate in similar relationships by funding OSS development and potentially even contributing to projects themselves, setting an example that may spur other large entities to act in kind.

The similarities between water management systems and OSS, including directional dependence, complex webs of intermediaries, and the need for sustainable usage, suggest a paradigm for policymakers weighing potential engagement with the open-source ecosystem. Considering directional dependence prompts a more accurate understanding of the importance of intermediaries in OSS as well as a better starting point for understanding the criticality of different OSS components and how to preempt costly incidents. Instead of expecting open-source software to be perfectly stable, well-maintained, and fully secure upon import, OSS consumers can continue to take more responsibility for their usage and all its benefits, consequences, and attendant obligations. Considering those connections also emphasizes the existing network of intermediaries between developer and end user, which government must engage with rather than disrupt. Finally, the water-management comparison emphasizes that a sustainable ecosystem requires a proactive relationship between large users and the source; an affirmative responsibility to contribute back to the ecosystem. Organizations with high expectations for, and dependence on, OSS be they public or private sector should devote substantial resources to supporting the relevant communities in meeting those expectations. Failure to do so will leave the OSS ecosystem perpetually under-supported and increasingly unable to support more complex and systemically critical use cases. The notion that open source might become unsustainable because of such overuse, or integration to critical applications without responsible consideration, would imperil the benefits of OSS to all.

NEVADA WATER LEGISLATION: MANDATE RESPONSIBLE USE

Regulations surrounding water use, allocation, and sustainability in the United States are largely the purview of states or multi-state consortiums.[54] Even where the federal government does take a more active role in water safety standards, such as with the Clean Water and Safe Drinking Water Acts, considerable room for state governments to take the lead exists, by design.[55] Water management legislation in Nevada, the country's most arid state, offers two examples of policy vehicles well-suited to the OSS ecosystem: Senate Bills (SB) 47 and 74, both passed in 2017. First, in SB 47, Nevada adopted the stance that "it is the policy of this State…To manage conjunctively the appropriation, use, and administration of all waters of this State, regardless of the source of the water."[56]

From the OSS perspective, this is a straightforward acknowledgment of how usage drives criticality—that, regardless of the source of code or water, **effective policy lies in governing where and how software is consumed as much or more than how it is developed**. In this sense, for OSS particularly, policymaking that takes the existence of OSS as it is rather than aiming toward an unrealized ideal for the code itself is useful, and it is particularly well met by Nevada's situation, whose primary sources of water generally originate in other states.[57] SB 74 offers more concrete guidance, requiring water suppliers—here, analogized to OSS intermediaries—to develop water conservation plans,[58] with some additional requirements for larger providers.[59]

Both SB 47 and SB 74 put a large burden for the sustainability of the state's water use on intermediary water suppliers—ostensibly those pulling water from its sources and sending it to users for various "municipal, industrial,

[53] "Open Source Security Foundation Raises $10 Million in New Commitments to Secure Software Supply Chains," Open Source Security Foundation (blog), October 13, 2021, https://openssf.org/press-release/2021/10/13/open-source-security-foundation-raises-10-million-in-new-commitments-to-secure-software-supply-chains/.

[54] "Water Law Overview - National Agricultural Law Center," National Agricultural Law Center, accessed January 12, 2023, https://nationalaglawcenter.org/overview/water-law/.

[55] "Drinking Water Laws and New Rules," Overviews & Factsheets, US Environmental Protection Agency, accessed January 12, 2023, https://www3.epa.gov/region1/eco/drinkwater/laws_regs.html.

[56] Pub. L. No. SB47 (2016), https://www.leg.state.nv.us/App/NELIS/REL/79th2017/Bill/4675/Text.

[57] Daniel Rothberg, "Everyone in Nevada Is Talking about Water. Here Are Five Things to Know.," *Nevada Independent*, May 19, 2022, https://thenevadaindependent.com/article/everyone-in-nevada-is-talking-about-water-here-are-five-things-to-know-efbfbc.

[58] To the reader, though originally required in the 90s, it is more precise to say that this legislation updated the requirements for those plans among other related items.

[59] Pub. L. No. SB74 (2016), https://www.leg.state.nv.us/App/NELIS/REL/79th2017/Bill/4728/Text.

and or domestic purposes" downstream.[60] For OSS, this compares with ensuring responsibility lies with those who take open-source packages and use them in downstream applications, rather than expecting the river of OSS itself to be clean and self-sustaining to a degree sufficient for uses outside its control (or even on the repositories, similar to aquifers and reservoirs here). These bills focus on water suppliers not just as the users of the resource but the intermediaries with much sway over the connective infrastructure, specifically calling out their role in developing "standards for water efficiency for new developments" and reducing leaks among other provisions.

There is no shortage of OSS,[61] but insofar as conservation serves as a synonym for sustainable use, federal OSS policy can draw on this framing. A policy pivot away from just assessing the risks of using OSS—say as required by many conventional supply chain risk management programs—and toward broader models of enforcing responsible use might include recommending an explicit Sustainable OSS Usage Plan as a signal of large OSS users interacting responsibly with the ecosystem, inclusive of managing their risk posture but also deliberate, systemic efforts to identify and support communities around critical OSS dependencies. There is much to be gained in shifting the focus of OSS policy to improve security from the developers and their code ("the source") to the framing of aggregate usage, reliance, and responsibility.

Moreover, the specific requirements of the Nevada conservation plans amount to a call for suppliers to explicitly understand their place and role in the larger ecosystem. Regarding intermediaries, more policies both from government and industry might focus on the ability of large code-hosting platforms to leverage their platform as natural bottlenecks in the ecosystem (as the means for many to access repositories and store their code) to provide useful tooling at scale to OSS communities. Some of this work is underway, and this is not a claim that it is insufficient but rather a call for policy to capitalize on those points of outsized returns on tooling investment and integration. Importantly, this is not a call for platforms to be responsible for the safety of all the code they host, but rather useful in the distribution and usability of tools to projects—to provide tools and capability for responsible use and security conscious development. In line with the water analogy, consideration of the context of different use cases is key—just as water powering hydroelectric dams need not be drinkable, different use contexts imply different support obligations and maintenance standards.

GOOD SAMARITAN INITIATIVE: LIMIT LIABILITY FOR VOLUNTEERS

Federal water law, meanwhile, has useful models for encouraging external support for the OSS ecosystem—specifically, unmaintained dependencies. The Environmental Protection Agency's Good Samaritan Initiative helps facilitate the cleanup of abandoned mines, a significant source of water pollution, with over half a million abandoned mines estimated throughout the country.[62] Volunteers assist in the cleanup of these abandoned mines, providing a great benefit to their communities, which often rely on the same water impacted by the pollution. The Good Samaritan guidance protects those volunteers explicitly from liability for their efforts, effectively lowering the bar to entry for helpful ecosystem contributions. Some federal programs go further by directly funding cleanups of water systems, though these often come within larger spending packages rather than pulled from specific funds.[63]

There are two OSS parallels here: unmaintained projects, and organizations doing support work (e.g., security auditing or incident response support). On the former, a Tidelift study in 2019 found that between 10 and 20 percent of common OSS packages lacked active maintainers, posing obvious security and sustainability challenges, and arising likely as a symptom of limited developer time and resourcing.[64] Organizations that support OSS projects are just an extension of this parallel beyond the common language of abandonment.

Government and industry might help improve the overall OSS ecosystem's health through incentives for Good-Samaritan-style engagement and by continuing to maintain the widely understood protection for OSS developers and maintainers against liability arising from the downstream uses of their components. This comparison points

[60] Pub. L. No. SB74 (2016).

[61] To the reader, one might argue that there is a shortage of OSS tailored to meet all consumers' needs, which leads to its constant change.

[62] "Fact Sheet: Good Samaritan Administrative Tools," US Environmental Protection Agency, accessed January 13, 2023, https://www.epa.gov/enforcement/fact-sheet-good-samaritan-administrative-tools.

[63] Rep. Lori Trahan (D-MA-03), Press Release: "House Passes Comprehensive Legislation to Aid Ukraine, Invest Millions in Third District," March 9, 2022, https://trahan.house.gov/news/documentsingle.aspx?DocumentID=2411.

[64] Havoc Pennington, "Up to 20% of Your Application Dependencies May Be Unmaintained," Tidelift (blog), April 9, 2019, https://blog.tidelift.com/up-to-20-percent-of-your-application-dependencies-may-be-unmaintained.

to the importance of policymakers vetting proposed policies relating to security requirements for OSS to ensure they do not create additional compliance-related liability for OSS developers, contributors, or maintainers, which might paradoxically deter individuals and organizations from contributing to the OSS ecosystem.

In addition to liability protection, an OSS policy equivalent could emphasize broader support and investment by funding external support groups (much of which already takes place through the private sector), guiding them toward critical under- or un-supported projects, and rewarding and aiding the "adoption" of orphaned projects still in use. There has already been some consideration of these approaches outside the public sector, such as the Alpha-Omega project and several academic studies[65]—providing the basis less for reinvention than for renewal of government support as part of a broader engagement with the OSS ecosystem.

Environmental regulations, including water management systems, in the EU are guided by the "polluter pays principle," which states that polluting entities should be responsible for costs like pollution control and prevention.[66] The principle encompasses a wide variety of regulations targeting different industries including agriculture and manufacturing. The types of cost for which polluters are responsible also vary, funding anything from cleanups of pollution they caused to investigations and permitting efforts. The principle is explicitly included in several important pieces of regulation, such as the Water Framework Directive and Waste Framework Directive.[67] Not all regulation is in line with the principle yet, but its inclusion in recent regulatory efforts and role guiding future policy demonstrates the EU's emphasis on ensuring that those who use natural resources, resulting in their degradation, pay for the consequences of their actions so the public need not foot the bill.

3.2.2 Capital Markets

A critical feature shared between financial markets and the open-source community is that both liquidity and OSS act as enabling inputs to a wide variety of other industries. Financial backing and loans from investors enable businesses and individuals to raise capital to overcome initial fixed costs, which is vital for getting businesses off the ground. Similarly, OSS allows businesses and individuals to save vast amounts of time and effort that would otherwise be spent re-solving similar problems—a critical input that helps overcome burdensome upfront investment. This enabling-input characteristic is true of many forms of physical infrastructure—in water management systems as noted above, as well as power grids, gas pipelines, transport networks, and more.

Capital markets, however, highlight the relationship between risk and transparency. In capital markets, debt or equity in real-world assets, stocks in companies, and mortgages back numerous financial instruments. Financial actors can manage their risk only by understanding the valuation and risk of these underlying components, and there are many intermediary entities such as ratings agencies that help create and provide this information. The 2008 financial crisis serves as a useful reminder of the consequences of failures in this system—when ratings agencies inaccurately appraised the risk of mortgage-backed securities, huge portions of the financial sector were left holding fundamentally unsound investments believed to be low-risk, leading to disastrous, global consequences.[68] Without accurate transparency, sources of systemic risk went unidentified, unaddressed, and unmitigated, fueling a financial meltdown.

There are useful parallels for the OSS ecosystem here. Like financial instruments, OSS often serves as the building blocks for other end products. For consumers

[65] Théo Zimmermann and Jean-Rémy Falleri, "A Grounded Theory of Community Package Maintenance Organizations-Registered Report," CoRR 2108.07474 (September 2021), https://dblp.org/rec/journals/corr/abs-2108-07474.html?view=bibtex; Jailton Coelho et al., "Identifying Unmaintained Projects in GitHub," in Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, 2018, 1–10, https://doi.org/10.1145/3239235.3240501; Jordi Cabot, "Adopt an Open Source Project," Livable Software, September 21, 2018, https://livablesoftware.com/adopt-abandoned-open-source-project/; Alpha-Omega; Adopt A Project, GitHub, accessed January 13, 2023, https://github.com/jonobacon/adopt-a-project.

[66] European Commission, "Specific Principles: Polluter Pays Principle," Principles of EU Environmental Law, https://www.era-comm.eu/Introduction_EU_Environmental_Law/EN/module_2/module_2_11.html.

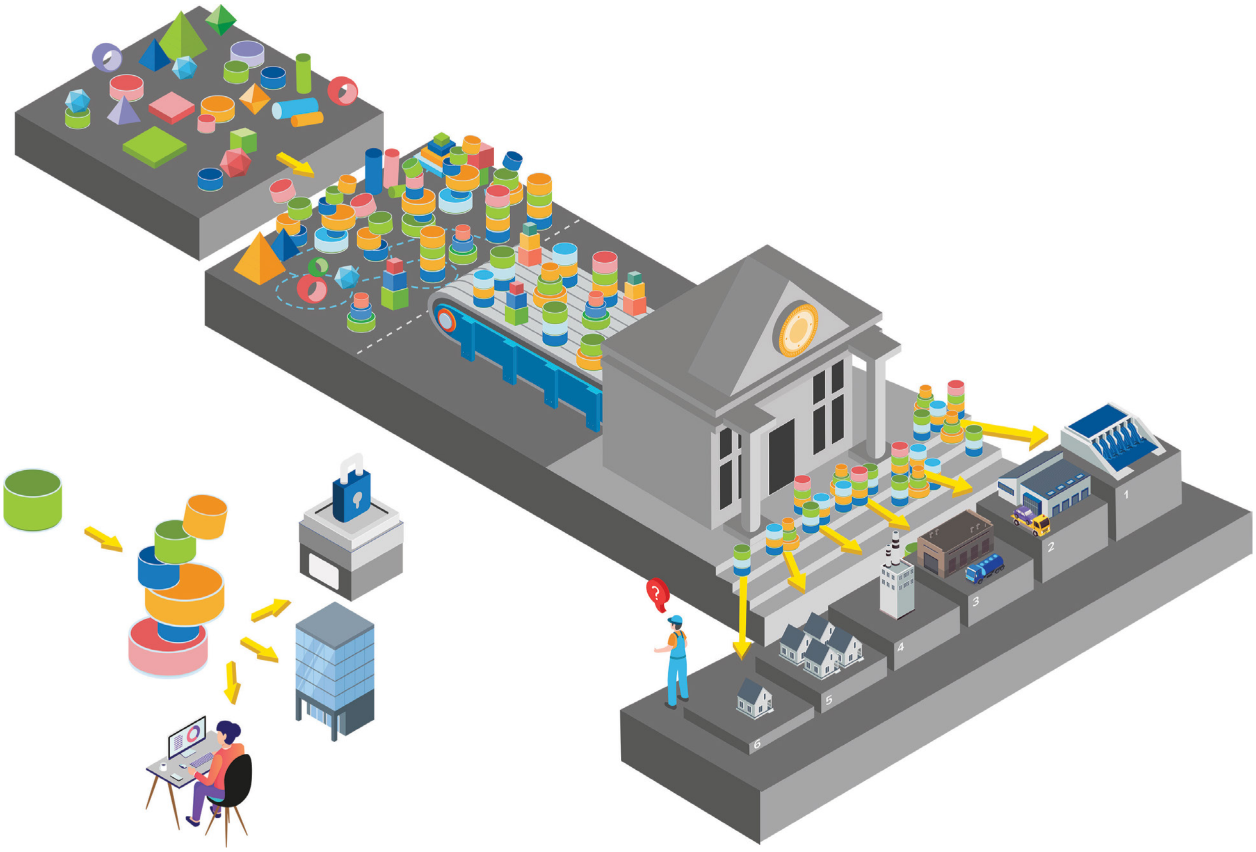
[67] "Waste Framework Directive," European Commission, https://environment.ec.europa.eu/topics/waste-and-recycling/waste-framework-directive_en and "Water Framework Directive," European Commission, https://environment.ec.europa.eu/topics/water/water-framework-directive_en.

[68] United States: Financial Crisis Inquiry Commission, "The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States" (Washington DC: US Government Printing Office, February 25, 2011), https://www.govinfo.gov/app/details/GPO-FCIC.

and producers, visibility into these components is necessary to improve risk-management practices. The entity that assembles a bundle of financial instruments—or a bundle of software that includes OSS components—holds a better perspective than the end user to understand the risks, as well as to know how to manage that risk through investment in upstream packages and projects. More transparency from assemblers can help recipients better understand the components within a product or a project and adjust their incident response and risk-management practices accordingly. The financial sector has developed procedures for assessing and describing risk, due to a combination of regulation, profit motive, and market demand. Industry-led development on tools and data to enable visibility into the use of OSS and other software components are already underway—software bills of materials (SBOMs) offer point-in-time insight into the components in a given piece of software (including open-source components), and ratings systems and metrics platforms like Supply chain Levels for Software Artifacts (SLSA), Community Health Analytics in Open Source Software (CHAOSS), and Open Source Security Foundation (OpenSSF) Scorecards offer aggregated insight into the security posture and maturity of those component projects.

At the systemic level, transparency and visibility into the use of OSS components can highlight where the wider digital ecosystem is leveraged on a small number of critical packages, helping to prioritize support and investment on all fronts. Heartbleed, the left-pad incident, and log4shell illustrate this kind of risk—where disruption in a single upstream component has widespread effects, and in some cases, deep ones.[69] The Census II report from

Figure 9. Capital markets and open source



[69] To the reader, examples include Heartbleed and log4shell.

the Linux Foundation and the Laboratory for Innovation Science at Harvard offers an example of the benefits of such system-scale analysis. The report used aggregated software-composition-analysis (SCA) data to identify open-source components widely depended upon across industry[70]—notably, the report identified log4j, the library impacted by the log4shell vulnerability, as one of those widely used packages (after the incident, unfortunately).[71]

The comparison to the financial sector also offers a model for how government might interact with industry and the open-source ecosystem. As noted, the private sector is already developing many of the tools that will help address risk with transparency. Government's role in that space is best understood as one that supports and provides appropriate incentives, especially for adoption over prescription—for example, through its procurement policies, rather than supplanting these tools or intensive regulation. As in financial markets, government is well-positioned to guide ecosystem-scale efforts toward a better understanding of aggregated risk concentrations. And, as with financial market data, government may also need to consider how to safeguard data collected for that analysis, which may have proprietary or trade-secret sensitivities. For OSS, a list of critical projects would be as useful to attackers in guiding their efforts as to defenders. Finally, at the most abstract level, the relationship between transparency and risk to the larger system can help guide broad government strategy, emphasizing that transparency and openness are not just rhetorical values but practical tenets of extreme, tangible benefit to the stability of the overall ecosystem.

FINANCIAL STABILITY OVERSIGHT COUNCIL: TRANSPARENCY TOWARD PROACTIVE STABILITY

Many proposed cybersecurity policies require a substantial level of system knowledge and data availability: they require being able to identify critical OSS packages across entities, the most significant users and beneficiaries of OSS, the overlap between projects that are unmaintained or under-resourced and that are key dependencies, and more. Policy vehicles from the financial sector, particularly those born out of the 2008 crisis, offer models for managing risk through transparency and an ecosystem-scale lens. Formed by the Dodd-Frank Act, the Financial Stability Oversight Council (FSOC) within the Department of Treasury works to "address several potential sources of systemic risk…[by] monitoring financial stability and designating…companies…and utilities as systemic[ally important]."[72] Where it identifies systemically important financial market utilities (FMUs), it can subject them to additional regulation in concert with the wide array of relevant government offices and regulators.

A parallel office for OSS would serve to identify projects, dependencies, and even entities that constitute systemically important infrastructure, and, in place of regulations, might offer those nodes of risk more targeted and comprehensive support, coordinating among government cyber authorities and industry, in place of financial regulators. Such a federal office would not need to limit its study to OSS dependencies. It could also contribute to analyzing cyber risk within other complex systems like cloud service providers and critical vendors to government.

Identifying points of risk concentration created by system-scale OSS dependencies points policy immediately toward the next mechanism from the financial system: **stress testing**. For financial entities, stress testing boils down, in part, to liquidity requirements—minimum asset-liability ratios meant to ensure institutional resilience to market shocks, or more simply having enough cash on hand to cope when things get ugly. For the OSS ecosystem, the first steps toward stress testing might include—once critical dependencies are better identified and understood—by-sector requirements for contingency planning in response to the compromise or degradation of important OSS packages. For example, government might start requiring such risk management of critical infrastructure sectors. This could also include exercises to respond to vulnerabilities in deep-in-the-stack packages or active compromise of developer tools or authentication systems widely depended on by identified software.

Critiques of the FSOC, and the larger Dodd-Frank Act (DFA) of which it is a part, illustrate useful considerations for a parallel body overseeing digital risk management concerning the OSS ecosystem. One notable concern

[70] To the reader, some companies offer as a service scanning of software products to identify with reasonable but varied accuracy the underlying components within.

[71] Frank Nagle et al., "Census II of Free and Open Source Software — Application Libraries," [Linux Foundation, Laboratory for Innovation Sciences at Harvard (LISH), and Open Source Security Foundation (OpenSSF), March 2, 2022], https://lish.harvard.edu/publications/census-ii-free-and-open-source-software-%E2%80%94-application-libraries.

[72] Jeffrey M Stupak, "Financial Stability Oversight Council (FSOC): Structure and Activities," Congressional Research Services, February 12, 2018, (https://digital.library.unt.edu/ark:/67531/metadc1157125/, accessed January 13, 2023, University of North Texas Libraries, UNT Libraries Government Documents Department).

for the DFA was its potential to overburden banks—both compared to other parts of the financial system and compared to international banks not covered by the act—to their detriment.[73] Crucially for the OSS ecosystem, increasing burdens on open-source project developers and maintainers, already short on time and money, should be a non-starter for any policy. Given the principle that use (rather than the manner of construction) determines the criticality of an OSS project, any responsibilities added to existing regulation will better suit large vendors, and, even there, an OSS FSOC need not create further red tape. Rather, such an entity could focus on gathering data-—perhaps initially focused on the federal government's most essential digital systems, the process of which could provide insights used to focus later iterations with other entities such as industry-heavy critical infrastructure sectors.

Metric selection is a significant challenge when assessing the risk of OSS projects, requiring careful consideration of both factors that affect a project's capacity for secure development as well as the levels of dependence on that project across a vast digital ecosystem. When asked about the former, survey respondents for this report were generally split across answers, emphasizing the lack of consensus on key risk heuristics, though they did consistently devalue the number of sponsors, either corporate or individual that a project had and more significantly weighing project popularity, a history of recent vulnerabilities, and community size.

Focus on identifying risk concentrations, over mandating how to address and manage that risk, would also help a potential OSS FSOC equivalent navigate another concern it would share with its financial counterpart, namely, the complexity of the existing network of relevant authorities. The web of federal financial authorities, not to mention the role states play in other portions of that sector, is a challenge for the FSOC to navigate.[74] Moreover, the division of powers and controls among federal cyber entities is even less mature. Many key agencies have come into existence only within the past decade. And unresolved and overlapping cybersecurity authorities in the United States remain divided between CISA, the Office of the National Cyber Director, the Office of Management and Budget, sector-specific agencies, chief information officers of agencies, and a variety of other offices and regulators at the federal and state levels. A digital FSOC's primary focus on information gathering and collation would avoid stepping on the roles and responsibilities of other entities while providing ecosystem visibility to help them regulate more effectively. A mission of identifying nodes of dependence would help avoid messy interagency conflict while still highlighting systemic risk and helping the federal government get its own (cyber) house in better order.

Operating similarly to the FSOC in the United States, the EU's European Services and Markets Authority (ESMA) oversees European financial markets. ESMA's four objectives are assessing risks, developing standards for financial entities, ensuring the consistent application of financial regulations across the EU, and directly overseeing specific kinds of financial entities. ESMA releases detailed reports on the European financial markets, with specific releases focused on various securities, derivatives, alternative investment funds, and retail investment products. Like the FSOC, ESMA was created in the aftermath of the 2008 financial crisis as regulators sought more insight into the interactions among complex financial instruments. ESMA focuses more on broader ecosystem risks across the European financial system than on subjecting certain companies or utilities to heightened scrutiny, in line with its advisory role.[75]

3.2.3 Roads and Bridges

The titular comparison of Eghbal's *Roads and Bridges* report links OSS to critical transportation infrastructure. The comparison draws out key characteristics of the open-source ecosystem, such as the free-rider dynamic and the necessity of consistent, mundane maintenance. The concept of usage driving the need for maintenance deserves particular focus. OSS is used in many varied contexts and is the backbone of most digital technology. Like interstate highways and other transportation infrastructure, open-source software inevitably require maintenance, and waiting too long to address emerging issues can result in a catastrophic incident down the proverbial road.[76] Responding to individual issues, like the collapse

[73] Walter Frick, "What You Should Know About Dodd-Frank and What Happens If It's Rolled Back," Harvard Business Review, March 2, 2017, https://hbr.org/2017/03/what-you-should-know-about-dodd-frank-and-what-happens-if-its-rolled-back.

[74] House Hearing 114th Congress: "Oversight of the Financial Stability Oversight Council" (Washington, DC: US Government Publishing Office, December 8, 2015), https://www.govinfo.gov/content/pkg/CHRG-114hhrg99796/html/CHRG-114hhrg99796.htm.

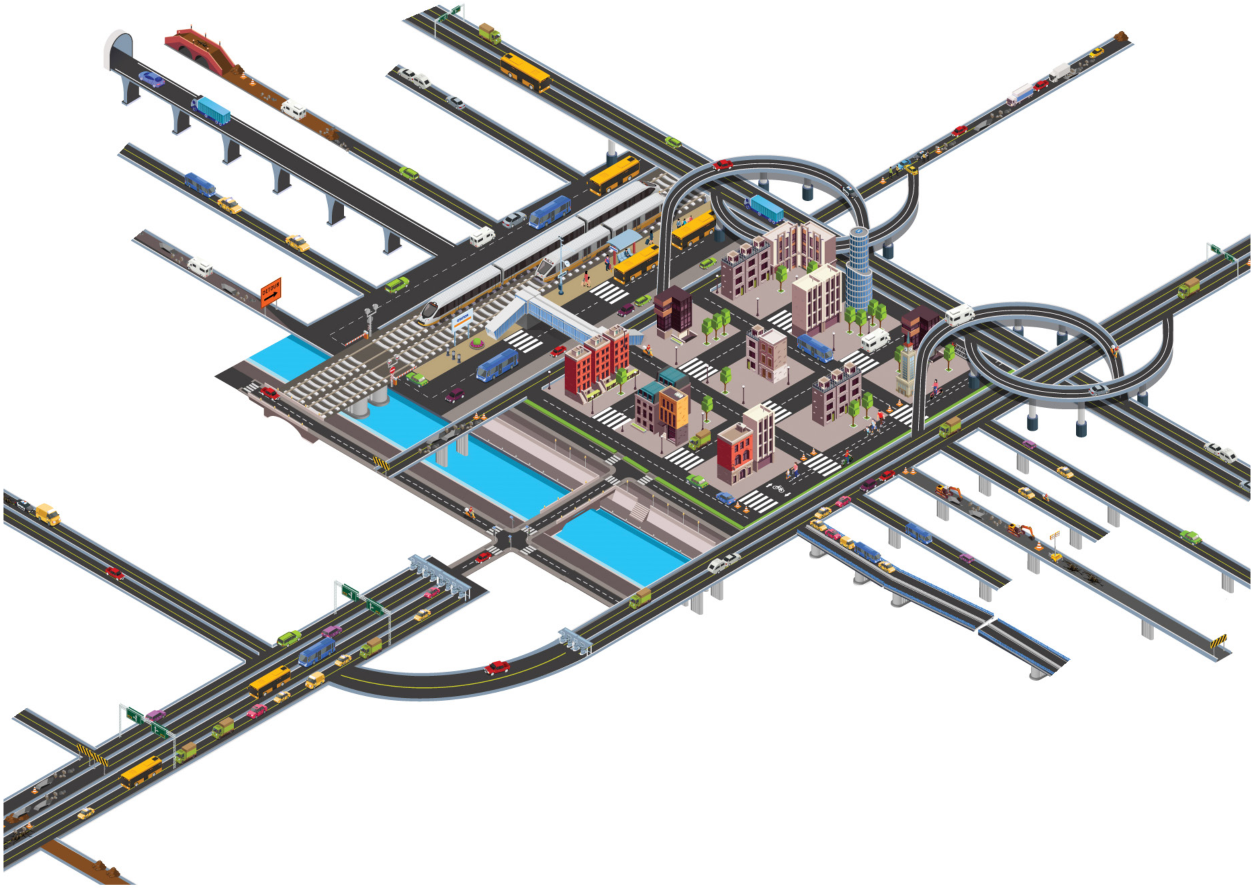
[75] "About ESMA," European Securities and Markets Authority, accessed January 13, 2023, https://www.esma.europa.eu/about-esma.

[76] To the reader, it is not the mere act of using code that creates the need for maintenance—binaries do not degrade like asphalt—but rather the fact that downstream dependencies and integrations make it essential for upstream components to keep pace with evolving language and environment features and security practices.

of a bridge or a widely-publicized vulnerability like log4shell, is essential, but is not enough to ensure the stability of the essential infrastructure of transportation systems or OSS. Coupling a recognition of OSS's essential nature with an understanding that most code is not static and will require additional support over time allows for targeted policies that address the crucial challenges of OSS ecosystems.

Relatedly, both physical transportation infrastructure and OSS ecosystems suffer from widely varying support, with no reliable transaction model to capture value from those who use the infrastructure and feed it back to maintenance and support. Eric Raymond identified this issue in *The Cathedral and the Bazaar* as a discontinuity between sale value and use value—the value of code at the point of transaction vs. its value in use over

Figure 10. Roads and bridges and open source



time.[77] Roads are costless to use outside of specific toll schemes and yet valuable to their users, especially when well surveyed and maintained. The widespread assumption of availability means that, without sufficient dedicated efforts to overcome this lack of support through consistent maintenance and funding, roads and bridges would collapse due to damage from use, while essential OSS components may degrade in availability or security as their developers fail to receive support commensurate with the criticality of their code.

The roads and bridges analogy also captures well the variety of use within the open-source ecosystem. In the same way that interstate highways receive more traffic than streets in suburban neighborhoods and some roads provide singular access to remote geographies, certain packages are critical due to either the large number of software packages dependent on them or their service of a particularly niche function, while other packages might be relatively less important to the ecosystem due to a lack of widespread use in downstream applications. Importantly, there is no singular way to use any OSS project—each can serve different users and applications differently, much like how roads rarely require or serve a single destination and are agnostic to the route of drivers.

Government has long worked to close resourcing gaps in transportation infrastructure, for example, through the Highway Trust Fund (HTF). While the exact nature of the most useful forms of support for OSS is up for debate—they might include any combination of funding, developer hours, tooling, security auditing, and more—government is uniquely resourced to bolster efforts in closing that gap and help reset market expectations for contribution by the private sector. None of this is to counter or dispute the original Roads and Bridges report. Rather, this report emphasizes the utility of its analogy of choice, adds others to capture different OSS traits, and below strives to connect extant transportation policy to workable OSS models. Figures 11 and 12 capture survey responses to questions on what methods of external support, and investment, for open source projects would be most useful, for open source maintainers/developers and downstream users respectively. The results are notably consistent across both questions, highlighting the link between upstream resources and downstream benefits.

THE HIGHWAY TRUST FUND: CONSISTENT AND SUSTAINABLE SUPPORT

For transportation systems, the HTF provides an example of consistent funding to maintain critical infrastructure. Maintaining transportation infrastructure requires preventative, systemic investment instead of reactive disaster response; the Highway Trust Fund provides financial support so that bridges do not have to collapse before they receive maintenance. As such, it provides a useful model for how to fund the maintenance of OSS.

HTF funding is spent largely through grants to state and local governments, suggesting the importance of working with existing entities within an ecosystem with regional expertise.[78] The federal government should not depend only on its own knowledge to identify useful recipients of funding—instead, it should work with industry and the existing web of OSS stakeholders including volunteer networks and paying foundations, relying on their expertise in the domain. Like the HTF, OSS funding could support instead of supplant existing efforts.

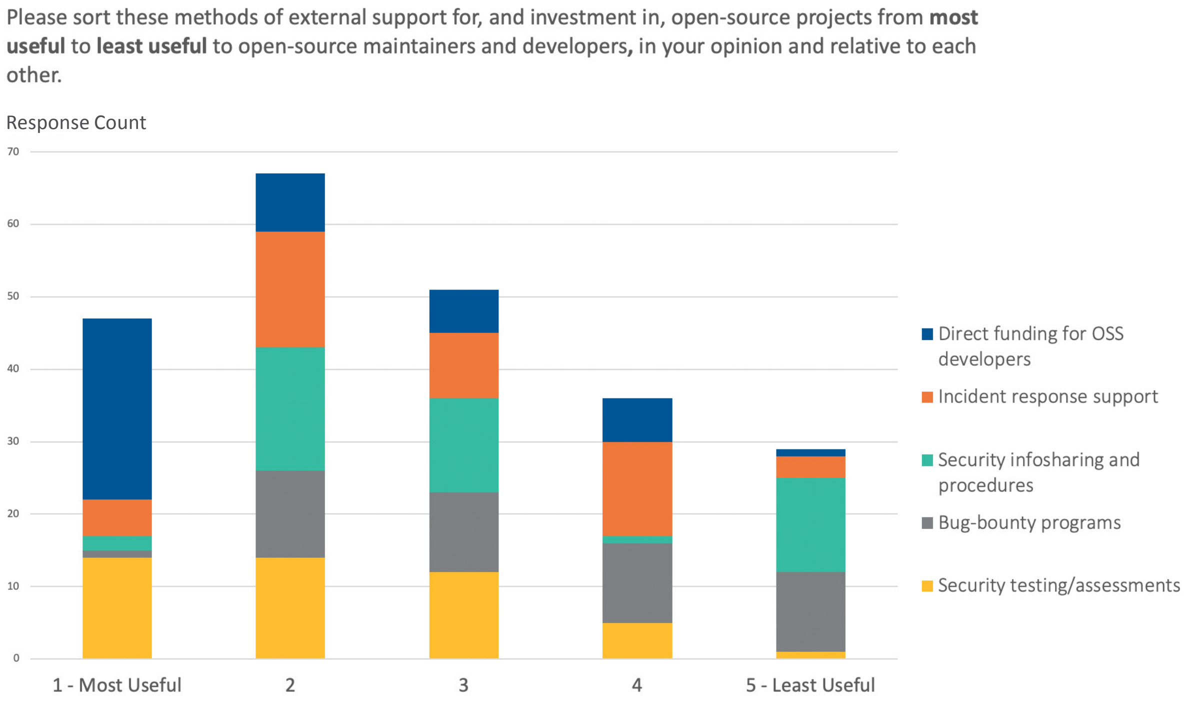
The HTF's explicit focus on construction *and maintenance* is also a model of a solution for a potential shortcoming in existing OSS funding: several previously mentioned examples of funding intermediaries tend to focus on investing in the development and creation of open-source solutions, but support is also needed for the long-term, less glamorous work of maintaining OSS projects—managing contributions, ongoing security engagement and community governance, and so on. The solution might look like a federal OSS Trust explicitly focused on backing extant projects rather than focusing on spinning up new ones. It might directly pay maintainers of critical projects, as well as support the development of tooling, security support organizations, and other scalable means to support a broader ecosystem of OSS components. Relatedly, survey respondents for this report prioritized tooling, with several specifically calling out automated, scalable solutions, and direct funding to OSS developers as most useful for both OSS project support and downstream security.

It is also worth mentioning the funding source that feeds the HTF: fuel taxes. From an economic perspective, the

[77] Raymond, The Cathedral & the Bazaar.

[78] "Highway Trust Fund: Federal Highway Administration Should Develop and Apply Criteria to Assess How Pilot Projects Could Inform Expanded Use of Mileage Fee Systems" (Washington DC: US Government Accountability Office, January 10, 2022), https://www.gao.gov/products/gao-22-104299.

Figure 11. Survey responses


Please sort these methods of external support for, and investment in, open-source projects from **most useful** to **least useful** to open-source maintainers and developers**,** in your opinion and relative to each other.

HTF thus linked (if by happenstance more than economic design) two distinct policy vehicles: a taxed negative externality and a subsidized public good. In a key difference from the HTF's fuel-tax funding, there is no clear negative externality for OSS usage, and policy should not aim to discourage its use. Instead, it should develop incentives for more responsible usage, such as tax credits for upstream contributions and donations to an OSS fund. Such a model for OSS, a fund supported by consistent contribution premised on use value, would offer another incentive lever for policymakers to encourage large OSS consumers to contribute back to the sustainability of the ecosystem, and could potentially encourage additional industry players heavily reliant on OSS but outside the IT sector to play an increasing role in supporting OSS. These entities might rely just as much on OSS as IT vendors but struggle to mature their own OSS programming and therefore benefit from more general means of upstream support.

ADOPT-A-HIGHWAY: INCENTIVIZE DIRECT LOCAL SUPPORT

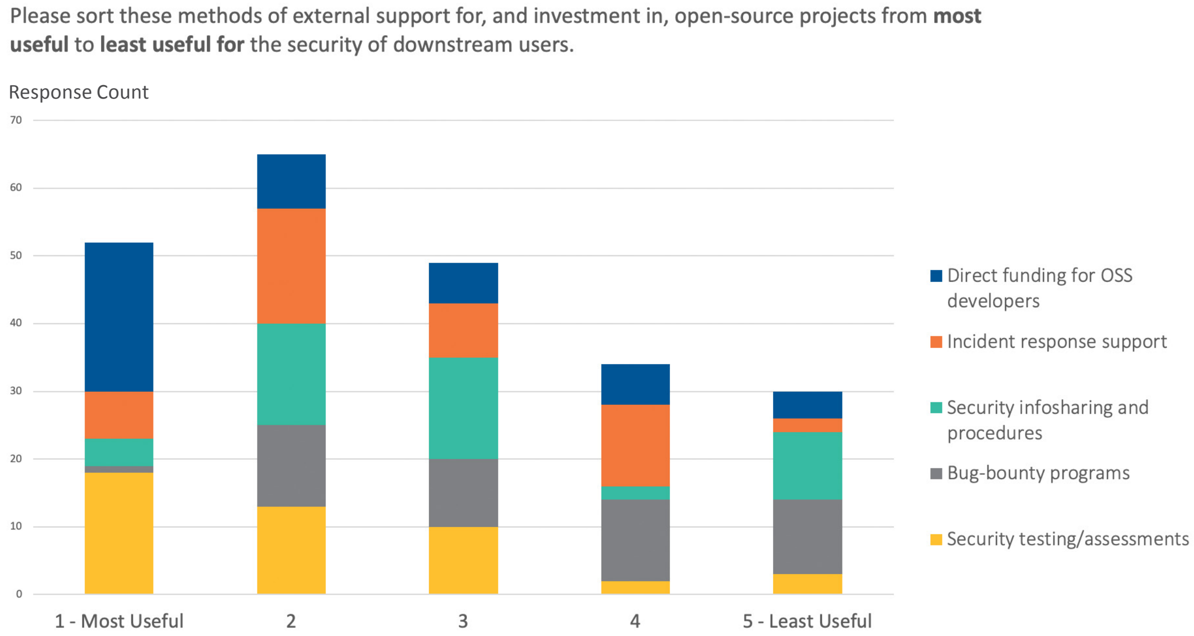
Transportation policy also provides a useful model for community-specific support. Adopt-a-highway programs are usually state-run endeavors connecting volunteers with stretches of local roads to remove litter. Aside from the convenient marketing phrase—adopt a package[79]—programs linking volunteers to both funding and packages they rely on and benefit from supporting offer another investment vehicle.

Adopt-a-Highway programs have faced challenges with groups seeking to participate in such programs.[80] While parallel lessons are not as direct here as with the HTF, it is worth clarifying the role of any potential adopt-a-package programs (AAPPs) in OSS. One long-running concern for OSS communities has been the role of large corporations in the governance and direction of open-sourcing products, potentially keeping features behind a paywall with forked proprietary code or swamping

[79] Adopt A Project.

[80] Lindsey Bever, "KKK Takes Adopt-a-Highway Case to Georgia Supreme Court," Washington Post, October 26, 2016, sec. Post Nation, https://www.washingtonpost.com/news/post-nation/wp/2016/02/23/kkk-takes-adopt-a-highway-case-to-georgia-supreme-court/.

Figure 12. Survey responses



Please sort these methods of external support for, and investment in, open-source projects from **most useful** to **least useful for** the security of downstream users.

independent projects with their sheer volume of contribution.[81] While the appeal of adopt-a-highway programs often lies in the optics of supporting local infrastructure, AAPPs can have a more practical purpose—they should instead focus on enabling and regularizing vendors substantively supporting the OSS projects they rely on, a practice already practiced in some isolated examples in the IT industry, with public recognition a secondary concern. There is a material benefit to these kinds of relationships, from component familiarity to better- managed and -resourced projects. Moreover, any implementation should healthily delegate to industry, which can better identify what projects require support.

Challenges that the HTF and adopt-a-highway programs have encountered can help pave a path forward for similar investment in the OSS ecosystem. The HTF, funded mainly by fuel-tax proceeds, has faced solvency crises requiring congressional intervention.[82] Concerns about the source of funding are pertinent to any potential federal OSS fund. Fortunately, some key differences between OSS and physical infrastructure help here. Road construction is slow and disruptive, but maintenance of OSS projects and support for their developers less so in helping with popularity of investment. While ROI studies for OSS and highways are somewhat spotty, the estimates for OSS ROI are promising if realized,[83] in addition to the knock-on benefits such investment might provide to national security concerns, workforce shortages, and more. Meanwhile, some OSS incidents can be directly connected to shortcomings in support,[84] from unpaid developers pulling down widely used packages to small teams challenged with vulnerability identification and remediation at scale.

[81] Morten Rand-Hendriksen, "On the Corporate Takeover of the Cathedral and the Bazaar," MOR10 (blog), February 4, 2019, https://mor10.com/on-the-corporate-takeover-of-the-cathedral-and-the-bazaar/.

[82] Committee for a Responsible Federal Budget, "The Infrastructure Bill's Impact on the Highway Trust Fund," CFRB, February 3, 2022, https://www.crfb.org/blogs/infrastructure-bills-impact-highway-trust-fund.

[83] Frank Nagle, "Why Congress Should Invest in Open-Source Software," Brookings (blog), October 13, 2020, https://www.brookings.edu/techstream/why-congress-should-invest-in-open-source-software/.

[84] To the reader, wording considers both security lapses and wider incidents where developers pull down packages. See: "Awful OSS Incidents" (2022; PayDevs), accessed January 12, 2023, https://github.com/PayDevs/awful-oss-incidents for examples.

Finally, while valid concerns about investment in transportation projects leading to government "picking winners" exist,[85] the OSS ecosystem indeed already has winners—projects meriting investment by virtue of either their ubiquity, criticality, or both—and there is much benefit to security in identifying those projects to begin with, as noted above. Moreover, the extant field of governance and support infrastructure from industry, nonprofits, and philanthropy already prioritizes some projects and modes of support over others—by necessity and often with more expertise and domain-specific knowledge than currently available to the federal enterprise. Working with and through those entities, rather than in parallel or at odds with them, and focusing on support and maintenance as much or more than project creation is a promising avenue for avoiding the lived shortfalls of some physical infrastructure planning.

These tangible policy vehicles all aim to make the three OSS as infrastructure analogies more readily useful, adding concrete intervention models and consideration of past challenges to the guiding principles and high-level characterizations of the OSS ecosystem already provided. The following section discusses a sampling of existing or proposed initiatives for policy engagement with the OSS ecosystem before converting the analogies into direct recommendations, primarily for government with some items including significant public-private coordination or giving the reins to industry.

Outside the United States, transportation infrastructure also faces a disconnect between the assumption of availability and the lack of support from those depending upon it. To overcome this gap and ensure essential infrastructure is maintained and reliable, the EU has several large funds that provide grants to build or maintain roads and other components of the transportation system. The Connecting Europe Facility (CEF) targets cross-border transport infrastructure, while the Cohesion Fund (CF) provides additional funding to countries in the EU with a Gross National Income per capita below 90 percent of the EU average. These funds help create consistency across the transportation infrastructure of the EU's member states—difficult to ensure without a coordinating central entity. The CEF and CF are part of the EU's sustainable development efforts, with both funds committed to ensuring that the infrastructures they build and maintain are energy efficient and cause minimal environmental impact. Though they spend toward slightly different project sets than the HTF—for example, the CEF also supports telecommunications and energy projects—the underlying principle is the same: infrastructure projects generally do not arise sufficiently from industry alone.[86]

[85] Hearing [archived webcast]: "Equity in Transportation Infrastructure: Connecting Communities, Removing Barriers, and Repairing Networks Across America," US Senate Committee on Environment and Public Works, May 11, 2021, https://www.epw.senate.gov/public/index.cfm/2021/5/equity-in-transportation-infrastructure-connecting-communities-removing-barriers-and-repairing-networks-across-america.

[86] "Cohesion Fund Fact Sheet," European Parliament, https://www.europarl.europa.eu/factsheets/en/sheet/96/cohesion-fund, and "Connecting Europe Facility," Innovation and Networks Executive Agency, December 22, 2022, https://wayback.archive-it.org/12090/20221222151902/https://ec.europa.eu/inea/en/connecting-europe-facility.

4

REAL-WORLD INFRASTRUCTURE POLICY FOR OSS

The open-source ecosystem and its many stakeholders have long recognized the need for sustained, stable support to projects and responded with the creation of nonprofits and institutions to provide that. Government support, tailored to both community needs and government priorities such as security or innovation, can provide robust, stable backing for the existing patchwork of organizations and projects in the OSS world. This section describes several existing policies for governments to take inspiration from and work with rather than assuming the whole burden of reinventing the wheel of OSS policy.

This section samples relevant policies—sourced principally from the Center for Strategic and International Studies' (CSIS) newly updated dataset, Government Open Source Software Policies[87]—in three categories synthesized from the three analogies above: government support and funding, ecosystem risk practices, and responsible use by OSS consumers. The CSIS dataset also described other kinds of policy outside these three categories—some establishing offices within governments dedicated to managing various OSS functions, often termed Open Source Program Offices (OSPOs), some requiring the open-sourcing of government-developed data and solutions, and others describing procurement practices.

4.1 Government Support and Funding

Policies establishing government support and funding for OSS were the most common of the three categories discussed here from the CSIS dataset, though there were still relatively few instances of these compared to the many procurement advisories and requirements it contained. Support for open-source projects in many ways is a natural extension of several government priorities—a search for non-proprietary solutions, support for acquired systems, and the logical conclusion of education and training programs—so their relative abundance makes sense. However, the fact that more policies discuss OSS procurement than OSS support is telling—just as in industry, it seems that governments are using OSS more than they are contributing back. The reasons for usage

[87] Eugenia Lostri, Georgia Wood, and Meghan Jain, "Government Open Source Software Policies," *Center for Strategic and International Studies*, January 10, 2023, https://www.csis.org/programs/strategic-technologies-program/government-open-source-software-policies.

are often clearly laid out: “to reduce the dependency on proprietary software,”[88] to reduce costs,[89] and to improve interoperability. Approaching OSS as infrastructure adds depth to this discussion—there are great benefits to using OSS solutions (and recognizing the vast majority of proprietary code incorporates OSS as well) and that usage creates a need to support the underlying projects. Though government support lags government usage, there are some models of supporting OSS projects—even those not acquired and used by government—that can help create the increased market choice so many procurement policies seem to desire.

In Germany, several organizations work to channel government funding toward OSS projects. The German Ministry for Economic Affairs and Climate Action funds Germany’s Sovereign Tech Fund, which launched a pilot round for funding open digital infrastructure in October 2022,[90] and the Prototype Fund which supports public interest technology—requiring that it be made available under open-source licensing—with investment coming from Germany’s Federal Ministry of Education and Research.[91]

There are nascent efforts in the United States too: the National Science Foundation’s Pathways to Enable Open-Source Ecosystems solicitation program launched in May 2022 to support governance organizations at the ecosystem level.[92] The Open Technology Fund receives funding from the US Agency for Global Media among other entities, part of which goes toward “advancing global Internet freedom” through supporting open-source projects relevant to its mission.[93] NASA's Open-Source Science Initiative funds and adjusts policies to encourage open and collaborative scientific processes, including through supporting open-source software and related infrastructure.

More broadly across the world, a 2013 Argentinian policy established a fund with over $2 million in initial backing to build OSS projects.[94] The Austrian government, in 2016, offered prizes of up to €200,000 for the OSS projects in various categories—the first round of funding shelled out €3.6 million across 31 projects.[95] One fund in Malaysia, set up in 2003, allocated $36 million for start-ups developing OSS, but further information on the project is scant.[96] These funds often support the establishment of OSS projects fulfilling an established need. While the support is generally useful, it is worth noting that as important as funding project creation is, supporting existing projects, in the long run, is even more vital to the long-term sustainability of the ecosystem.

4.2 Ecosystem Risk Management

Though no government policies in the dataset explicitly focus on assessing ecosystem-wide risk in the OSS world, interest in dedicated open-source offices provides a possible avenue toward this activity. Recently, governments have begun turning an eye toward formal offices dedicated to the many open-source activities they may undertake, such as project support, license compliance, security evaluation, incident response, public awareness, and providing clear points of contact for government employees and OSS developers. These OSPOs originate in industry as departments for coordinating all manner of open-source efforts.[97] The World Health Organization recently established an OSPO, for example,[98] and the European Commission’s Open Source Software Strategy for 2020–2023 includes establishing an Open Source

[88] Gijs Hillenius, “Norway to Increase Its Use of Open Source,” Open Source Observatory, November 19, 2008, https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/norway-increase-its-use.

[89] Federico Chiarelli et al., “Open Source Software Country Intelligence Report - Portugal” (Brussels: European Commission - Interoperability Unit, April 2020), https://joinup.ec.europa.eu/sites/default/files/inline-files/OSS%20Country%20Intelligence%20Report_PT_0.pdf.

[90] Sovereign Tech Fund, German Ministry for Economic Affairs and Climate Action, accessed January 13, 2023, https://sovereigntechfund.de/en.

[91] Prototype Fund, Open Knowledge Foundation Germany, accessed January 13, 2023, https://prototypefund.de/en/.

[92] Program Solicitation, NSF 22-572: “Pathways to Enable Open-Source Ecosystems (POSE),” National Science Foundation, https://www.nsf.gov/pubs/2022/nsf22572/nsf22572.htm.

[93] “Supporting Internet Freedom Worldwide,” Open Technology Fund, https://www.opentech.fund/.

[94] “The Ministry of Science Creates a Cluster for Free Software Companies,” iProfessional, April 26, 2013, https://www.iprofesional.com/tecnologia/159530-el-ministerio-de-ciencia-crea-cluster-para-empresas-de-software-libre.amp.

[95] Gijs Hillenius, “Up to EUR 200,000 for Austria… | Joinup,” Open Source Observatory, August 22, 2016, https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/eur-200000-austria.

[96] John Lui, “Malaysia Sets up $36m Open Source Fund - Silicon.Com,” Silicon, October 30, 2003, https://web.archive.org/web/20050411192233/http:/software.silicon.com/os/0,39024651,39116677,00.htm.

[97] Chris Anizczyk et al., “Creating an Open Source Program,” Open Source Guides, n.d., https://www.linuxfoundation.org/resources/open-source-guides/creating-an-open-source-program.

[98] Astor Nummelin Carlberg, “The WHO Is the Latest Public Administration to Launch an Open Source Programme Office,” Open Source Observatory, March 18, 2022, https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/who-builds-ospo.

Program Office within the commission to implement relevant OSS actions of the strategy.[99]

Other governments are focusing on information gathering. This year, the Japanese Ministry of Economy, Trade, and Industry released a report from a task force studying Software Security, which studied private sector reliance on OSS. Government initiatives that study the open-source ecosystem can provide crucial information which can then guide future investment and support of OSS.[100] Similarly, the proposed bill S.4913, the Securing Open Source Software Act of 2022, includes a requirement for the US government to conduct a study assessing its own reliance on OSS as well as its ability to accurately track those dependencies either through SBOM data, existing government programs like the Continuous Diagnostics and Mitigation (CDM) program run by CISA, and other sources of information.

4.3 Responsible Use

Policies that focus on patterns of responsible use in the OSS landscape were scant. One Armenian document concerning the country's principles of internet governance noted that the central role of decentralization in the development of the internet, specifically regulation on OSS, should be light, if necessary, at all.[101] Other instances of policy embracing the cultural values of OSS also exist, and the preference of governments to open-source their own solutions and code is notable. However, an explicit discussion of incentive and responsibility structures in the OSS ecosystem is somewhat lacking. Notably, White House conversations about the forthcoming National Cyber Strategy have not included any new mechanisms to explicitly support OSS, addressing little more than a carve out to protect OSS developers from any potential liability regime: a good and warranted item but underwhelming against the totality of need in the ecosystem.

While government policies for OSS exist, they focus more on the government as a consumer than as a regulator or supporter. Government procurement preferences seem driven by a desire for autonomy from large vendors and expensive licenses and patterns in little procedural upstream contribution. Though some funding models exist, by and large, government policies explicitly addressing OSS seem to focus on what government purposes it can serve and what transparent values it might inspire in government practice.

[99] Think Open, "Communication to the Commission: Open Source Software Strategy 2020 - 2023" (Brussels, October 21, 2020), https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/open-source-software-strategy_en.

[100] "Collection of Use Case Examples Expanded Regarding Management Methods for Utilizing Open Source Software and Ensuring Its Security," (Tokyo, Japan: Ministry of Economy, Trade and Industry, May 10, 2022), https://www.meti.go.jp/english/press/2022/0510_003.html.

[101] "Extract from the Minutes of the Session of the Government of the Republic of Armenia - On the Endorsement of Internet Governance Principles," http://www.irtek.am, August 2014, http://www.irtek.am/views/act.aspx?aid=77996.

5

CRAFTING INFRASTRUCTURE POLICY FOR OSS

OSS is really not much different from proprietary software: all code can be developed more securely, and the security risks OSS faces are common across most digital systems. For OSS the differences come in the relationships between open-source consumers—from government to the private sector to end users—and the projects they rely on. The lack of clear transactional relationships and the deeply influential role of the diverse, ever-changing contributor community are a challenge for policy and industry to navigate and support sufficiently. The result is an ecosystem that has both enabled digital innovation and often suffered from overburdened developers and under-resourced communities and projects.

5.1 Encouraging Sustainable OSS Participation

The recommendations of this section aim to use policy levers and industry collaboration to provide models for sustainable usage of and support for the OSS ecosystem, emphasizing responsibility driven by usage.

5.1.1 Start By Improving Government Consumption

In the United States, the federal government is not just a regulator but also an enormous consumer of OSS. This enormous use case provides a valuable opportunity for the federal government to test many of the recommendations below on its codebases, which is of immediate benefit to the federal enterprise. If the federal government is to truly assign as much importance to the OSS ecosystem as it has recently signaled,[102] it might consider **creating institutional entities with an explicit mandate to focus on the federal government's use of and support for OSS**, **modeled after OSPOs recently established by other organizations**. For the United States, a whole-of-government OSPO-like entity could be established within OMB or (with a focus on government procurement) the General Services Administration (GSA). Alternately, OMB and GSA could provide a coordinating function for smaller OPSO-like entities established in each agency. Such a program could take inspiration from the

[102] Dan Knauss, "Open Source Communities: You May Not Be Interested in CISA, But CISA Is Very Interested in You," Post Status (blog), October 3, 2022, https://poststatus.com/open-source-communities-you-may-not-be-interested-in-cisa-but-cisa-is-very-interested-in-you/.

OPEN Government Data Act, which requires the designation of Chief Data Officers within federal agencies,[103] by requiring agencies to designate a Chief Open Source Officer (COSO).

In addition to setting agency policy around the use of OSS and managing relationships with relevant OSS communities and vendors, agency COSOs could also contribute to a whole-of-government OSS strategy through a structure like an inter-agency Chief Open Source Officers Council, modeled after or housed within the Chief Information Officers Council. S.4913, if enacted into law, would pilot OPSO-like programs in the federal government by directing OMB to select agencies to create pilot OSPO-like entities to develop standards for their agency's use of OSS and engagement with the OSS ecosystem.[104] EU member states, where collaboration with the OSS community and consumption of OSS similarly need not tie as closely to cybersecurity regulators, could well replicate this model.

Regardless of whether they have an OSPO, or an existing commitment to OSS consumption and development, (in the United States, see entities like the Department of Defense (DoD) and National Aeronautics and Space Administration (NASA)), all agencies should also **encourage and fund travel to OSS community forums for government employees engaged with software development, procurement, and/or technology governance.** The social graph of a project defines OSS development, maintenance, and growth. The security of this code and its sustainable integration into government software projects would benefit greatly from wider government employee participation in the myriad conferences and governance bodies that populate the OSS ecosystem. While this may be a practical challenge for some defense and intelligence organizations, it is an important, meaningful way to integrate government needs and contributions more fully into OSS communities and help identify risks and opportunities for sustainable use.

5.1.2 Support Private-Sector Consumption

Develop an OSS Usage Best Practices framework through the National Institute of Standards and Technology (NIST) with significant industry input. Such a framework could include and build on the proposed OSS risk assessment guide recommended by S.4913.[105] However, it should also incorporate consideration of upstream contribution as a foundational measure of organizational maturity around OSS usage. Included among its recommendations should be an organizational plan for sustainable OSS use.

This document would serve as a reference for further policy attempts to incentivize investment in OSS sustainability. For example, government procurement processes could include consideration of for-profit vendor compliance with the NIST OSS Usage Best Practices framework. By framing compliance as a consideration rather than a hard mandate, the goal would be to incentivize for-profit providers without precluding nonprofit and individual contributors lacking the resources to develop a compliance program. A similar framework, which considers financial contributions to upstream projects, could help guide the application of tax credits used to incentivize donations.

Industry, as well, could take a leading role here, developing a common, voluntary OSS-engagement plan across entities under the auspices of a coordinating nonprofit such as OpenSSF. Important too would be including non-IT companies in these considerations. Though understandably less fluent in the technology sphere, large industry manufacturers and other corporations nonetheless have a considerable dependence on OSS projects. Where such large, non-IT companies have their own robust IT resourcing and capacity in-house, they too should build and contribute to models for risk management based on discarding the assumption of availability or functionality of critical OSS packages.

A NIST guide on best practices for OSS usage could also help guide federal developers and agencies in their relationships with vendors, key projects, and larger risk-management practices. Further, federal developers' and procurers' experiences with using such a framework could help inform future iterations of the document and bring industry best practices more fully into the federal enterprise.

5.1.3 Protect OSS Good Samaritans

Private-sector firms with existing investments in the open-source community (e.g., Google, Microsoft/GitHub, and

[103] "Foundations for Evidence-Based Policymaking Act of 2018," H.R.4174, 115th Congress (2018), https://www.congress.gov/bill/115th-congress/house-bill/4174.

[104] "Securing Open Source Software Act of 2022," S.4913.

[105] "Securing Open Source Software Act of 2022," S.4913.

IBM/RedHat) and well-established OSS governance and security organizations (e.g., OSI, the Open Source Collective, OpenSSF, and the Internet Security Research Group) should lead on drafting a best-practice standard for contributing to and supporting OSS projects. This document should help define the standard of care associated with volunteer contributions. This standard is not a form of liability protection but a way for firms to design policies encouraging volunteer contributions to OSS packages in a way that best meets corporate risk appetite. These volunteer commitments are an important way to contribute back to OSS used by companies and are a form of contribution-in-kind to support packages used by others.

5.2 Address systemic risk

The rapid pace of digital innovation and the informal relationships between OSS dependencies and their downstream beneficiaries has led to a digital ecosystem prone to stacking risk in a relatively small number of critical OSS projects, and created challenges for nonprofits, governments or companies seeking to obtain visibility into those points of concentration. These recommendations aim to align government and industry in systematically identifying key dependencies meriting direct support and investment without adding undue regulatory burden. These recommendations take inspiration from the FSOC and ESMA entities in the capital markets analogy.

5.2.1 Establish an Office of Digital Systemic Risk Management (ODSRM).

Modeled after the FSOC or ESMA described above, a central government office would, in close cooperation with industry and OSS community stakeholders, work to identify critical OSS dependencies both in the federal civilian agencies and across critical infrastructure sectors. This office might eventually mature from identifying these points of concentration to stress testing their compromise (either malicious or otherwise) and the related, wider ecosystem effects, modeling and exercising through variations on future log4shell-style events using real-world dependency information.

In the United States, this office should have broad authority to draw on federal expertise wherever it might reside, from the National Security Agency to CISA, and focus both on identifying specific critical OSS projects or systems and methods for producing and collating dependency data that can highlight nodes of risk. Such data might, for instance, include pooling SBOMs provided to government during its procurement processes. Given the large mandate this office would eventually assume, implementation might best start in pilot programs focused on mapping out the dependencies of one or more federal IT systems. Existing programs to map Federal digital assets and existing Federal vendors would be natural partners in the project. However, in the latter case, the implementing agency, perhaps with congressional support, would need to overcome obdurate industry resistance to the inclusion of dependency data about software products in the form of software bills of material, despite being regularly generated and consumed already. While the array of use cases for these SBOMs is still maturing,[106] large organizations, like New York Presbyterian Hospital,[107] already use them regularly. And there is a healthy supply of software tools to generate and process them employed by for- and nonprofit entities.[108]

Lessons learned from the analysis of one system could inform a widening aperture across other government systems and eventually across the broader digital domain, particularly considering that there may be significant overlap of key OSS dependencies between similar systems. Establishing an ODSRM is an opportunity for government to better map its own digital systems and assets before using lessons learned in that process to inform its approach to a larger, industry-wide attempt at helping to identify key critical dependencies.

5.3 Provide Resources with Security and Sustainability in Mind

Throwing funds at a problem is rarely ever a sufficient fix, but where investment shortfalls exist, it can help. These recommendations focus on guiding policymakers toward a resourcing model that helps cover funding gaps, particularly around long-term maintenance and support rather than the creation of new OSS projects, while accounting for non-financial resources (e.g. labor time, expertise) and

[106] Amelie Koran et al., "The Cases for Using the SBOMs We Build," *Atlantic Council* (blog), November 22, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-cases-for-using-sboms/.

[107] Katie Bratman and Adam Kojak, "SBOM Ingestion and Analysis at New York-Presbyterian Hospital" (Open Source Summit North America 2022, Austin, TX, June 21, 2022), https://ossna2022.sched.com/event/11Q0t/sbom-ingestion-and-analysis-at-new-york-presbyterian-hospital-katie-bratman-adam-kojak-newyork-presbyterian-hospital.

[108] To the reader, for more examples of SBOMs already for OSS projects, see the bom-shelter dataset built by John Speed Meyers and Chainguard: "bom-shelter" (Chainguard), https://github.com/chainguard-dev/bom-shelter.

financial support for important non-technical factors (e.g. encouraging contributor community depth and diversity, governance and good package management policies) and relying on community expertise in directing resources toward critical projects.

There are three important factors to consider in developing schemes for government support to OSS as infrastructure. First, where resources go is as important as how they get there. Direct funding and government-to-project contributions may work well for areas of urgent or existential need, but OSS projects will benefit most from consistent support delivered with local knowledge about the project, its maintainer community, and its user base. Few, if any, government-led schemes will be able to achieve this level of local knowledge on their own, so resources should mostly, flow through trusted intermediaries like software foundations (e.g., Apache, Linux, and Eclipse) and nonprofit groups (e.g., Open Source Collective and the Internet Security Research Group) as well as selected university programs.

Second, support must be sustainable. One of the difficulties of private-sector funding for OSS projects and their security is that, outside of a handful of exceptions, crisis has been the catalyst for much of this support. Monies flow to projects and project classes affected by an ugly vulnerability or momentary disaster without the promise of consistent, long-term commitment that project owners can plan and build around. The good work of several software foundations across the OSS ecosystem is a function of both the resources they bring and the stability they offer.

Third, it bears repeating that resources need not just be financial. Dollars and euros are fungible and necessary—volunteer labor can only bring OSS projects so far and might not account well for specific technical skills or experience needed to audit code or management and governance processes. Governments, generally, possess a scale of financial power available to few in the private sector. But governments also have other policy levers. Changes to government policy can reduce barriers to sustainable OSS adoption, open new opportunities for agency and government employee-level contributions back to OSS projects and punish abusive or malicious behavior targeting OSS communities. These are non-monetary contributions to the long-term security and sustainability of OSS and important alongside financial support.

With that in mind, this report offers three final recommendations on how to shape government support for OSS, keeping security and sustainability as the key goals, instead of massive feature expansion or redevelopment.

5.3.1 Target of Opportunity

Governments with the financial and organizational wherewithal should create target-of-opportunity funding programs to support OSS security. The goal of this funding is to award resources in a targeted manner, determined by government need, to OSS projects and activities. These awards should root in criticality and help account for urgent needs, ideally in anticipation of, but perhaps in response to, a crisis. Criticality can be determined by an entity, like the ODSRM, and used to guide single-agency or cross-government resourcing schemes. Smaller than the OSS Trust discussed below, a Target of Opportunity funding pool should scale into the single or tens of millions, allowing governments to resource security and compliance requirements that might fall on OSS programs as well as urgent mitigations and responses to incidents.

In the United States, such a program should be run by the federal agency best positioned to assess and respond to insecurity in technologies supporting critical infrastructure and broad swaths of society—CISA, under the US Department of Homeland Security (DHS). Congress, in S.4913, already views CISA as the logical home for tracking the use of OSS across the federal government and assessing the risks posed to OSS and other software. CISA should have the resources to support the implementation of those efforts and support the OSS projects identified as critical dependencies along the way.

5.3.2 Establish the OSS Trust

Recognition of OSS as the digital infrastructure underneath myriad economic and social activities entails a collective acknowledgment of the failure to-date to support it as such. Across national boundaries, open-source code generates and captures considerable value without consistent government backing, neither for the most critical security updates nor for long-running code maintenance and improvement. New resources will not solve every problem faced by OSS maintainers, and the intention of government support of this kind is not to rewrite the economic relationship between the maintainers of free and "as-is" code and their users.

The OSS Trust should be a mechanism for governments to provide consistent support for the security of OSS code, the integrity of OSS projects, and the health and size of OSS maintainer communities. These funds should scale into the hundreds of millions, enabling broad training and education programs, to support security reviews and mitigation for hundreds of projects at a time, and to bring more maintainers and contributors into OSS communities. These funds can help facilitate widely useful security research and cover the costs associated with long-term hardening, like rewriting a project in a memory-safe language. The Trust's thesis of what to support should center on activities that produce sustainable, long-term improvements as well as less-well-funded aspects of secure OSS projects like effective governance practices.

In the United States, **NIST could aid this effort by developing an inclusive list of metrics by which to gauge the health and needs of OSS packages and communities** in close cooperation with extant industry initiatives such as OpenSSF's Scorecard project, SLSA, S2C2F SIG, CHAOSS, and others.[109] It might focus on determining what best practices signal project maturity and sufficient resourcing, and what shortfalls are most critical for downstream users and thus worth prioritizing in upstream support. This framework should not supplant, but rather aggregate and synthesize extant industry measurement initiatives and could later be part of vendor assessments and best practices documents in government procurement processes.

In the United States, the OSS Trust should rely on both regular congressional appropriations and the diversion of a small portion of corporate taxes. Depending on the structure of the receiving organization, Congress could also consider incentivizing individuals and corporations to contribute to the fund or similar organizations through tax-credited donations. Given the immense room for improved support in the OSS ecosystem, such a fund need not begin at its final potential size, able to satisfy all needs at once, on the first day but can grow incrementally, taking the opportunities to refine its grantmaking processes and partner-organization relationships as it grows.

This can and should eventually be an international scheme. The German-government-backed Sovereign Tech Fund already works to fund OSS projects to "support the development, improvement, and maintenance of open digital infrastructure."[110] This and similar initiatives at the EU member state level could be subsumed into a broader international effort in the near future or grow in isolation and work to coordinate with U.S. and other national programs absent immediate consolidation.

Like the HTF, CEF, or CF, such a fund should work with intermediaries to identify the best recipients—the central government need not try to locate decrepit concrete and unaddressed potholes itself, but rather can improve the resourcing of organizations with that on-the-ground expertise, relying on the existing web of intermediaries and support groups already present and growing in the OSS ecosystem.

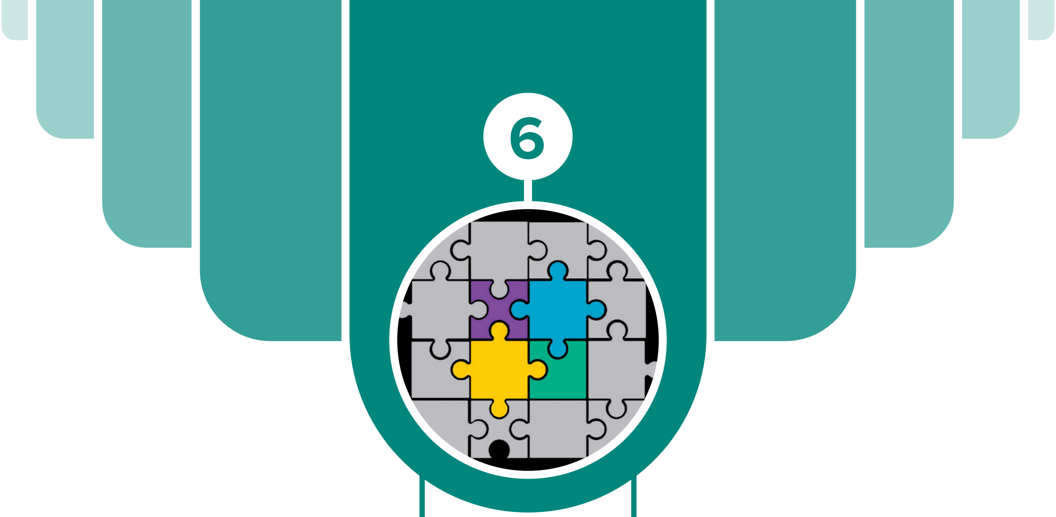
5.3.3 Adopt-a-Package

Private sector and nonprofit leaders in OSS should define schemes by which firms and other donors can "adopt" important unmaintained packages and provide resources to support their ongoing maintenance, vulnerability mitigation, and potentially rewrites into memory-safe languages or other structural updates. Rather than the urgent need met by a target-of-opportunity model or the long-term focus and friendliness to cross-cutting research of the OSS Trust. The government can contribute funding and support to existing initiatives or construct one in parallel, similar to Federal Emergency Management Agency's (FEMA) reservist program. Government teams might supplement private-sector groups or focus on assisting incident response and resourcing for projects critical to government functions.

One entity already working toward this end is the for-profit startup, thanks.dev, which looks to connect users and patrons of open-source packages with a simple way to fund those packages *and* the packages they depend on. The company builds on several layers of deep dependency graphs using existing bill-of-materials, like data. That part is crucial—because of the web of dependencies across OSS, funding standalone packages is often not enough to drive resources everywhere they are needed. Log4j is a great example of a piece of a whole that turned out to be extremely important in the aggregate but may not have attracted high-profile attention on its own.

[109] Open Source Security Foundation, "Secure Supply Chain Consumption Framework (S2C2F) SIG," GitHub, accessed January 11, 2023, https://github.com/ossf/s2c2f.

[110] Sovereign Tech Fund.



6

CONCLUSION

We do not build most of the code we use. In realizing this and accepting it for the indefinite future, OSS and the many communities developing and maintaining it should loom large in any analysis of cybersecurity and economic health. Open source constitutes the infrastructure to which we trust sensitive data, critical social programs, and cycles of economic development and innovation. That such infrastructure is weakening,[111] and in some places crumbling,[112] from the weight of demands placed on it should no more shock us than the imagery of bridges collapsing and reports of poisoned groundwater due to inadequate sustainment combined with widespread use.

None of this report reflects a belief that OSS is inherently insecure, but rather that it is uniquely central to modern digital systems and that relationships with the OSS community are necessarily, and substantively, different than those government has grown accustomed to with industry and industry within itself. Sustainable use emphasizes the user responsibility for much of the risk associated with software use, including OSS, and addresses OSS-specific features of development and contribution possibly only with open-source code. Addressing systemic risk is an important step for policy efforts to support the security and sustainability of OSS projects with an accurate picture of the considerable interdependency between code bases. Finally, governments must step up to support OSS as the infrastructure that it is. These resources should come alongside expanded private sector support and can manifest in targeted formats as well as a more general support model, the OSS Trust. OSS is infrastructure, and the provision of support for it as such will permit more rapid adoption and considerable innovation in even critical domains of economic and government activity.

Most of us too often take for granted the everyday things, the problems well solved. Yet, ignorance and the failure to protect them come with hefty price tags. Log4shell, a rash of open-source package incidents,[113] and the chorus of concern amongst OSS maintainers about an economic model that extracts value from labor without committing back are symptoms of the choice to remain in such ignorance. The risk is the slow collapse of a vibrant ecosystem and a future riven by falling diversity in and capability for digital development outside a concentrated handful of technology firms, imperiling national security and economic competitiveness in equal measure. The good news is that this collapse is neither necessary nor permanent.

Change is possible, indeed much needed, but it must come in the form of investment as well as policy. Pennies on the dollar of value can be gained from a healthy and resilient open-source ecosystem, and such investments provide a means to secure essential digital infrastructure against a myriad of threats. Strong investment in and well-informed policy about OSS is, above all, a gift to the present, not just an abstract donation to future generations, that would impact and protect communities throughout the world.[114]

[111] James Mcbride and Anshu Siripurapu, "The State of US Infrastructure," Council on Foreign Relations, November 8, 2021, https://www.cfr.org/backgrounder/state-us-infrastructure.

[112] Jim Mone, "NTSB: Design Errors Factor in 2007 Bridge Collapse," USA Today, November 13, 2008, http://usatoday30.usatoday.com/news/world/2008-11-13-628592230_x.htm.

[113] Dan Goodin, "Numerous Orgs Hacked after Installing Weaponized Open Source Apps," Ars Technica, September 29, 2022, https://arstechnica.com/information-technology/2022/09/north-korean-threat-actors-are-weaponizing-all-kinds-of-open-source-apps/.

[114] "OpenSSF Annual Report – 2022," Open Source Security Foundation, December 2022, https://openssf.org/wp-content/uploads/sites/132/2022/12/OpenSSF-Annual-Report-2022.pdf.

APPENDIX: SURVEY RESULTS

As part of this report, the Atlantic Council and the Open Source Policy Network distributed an anonymous survey to several OSS governance, policy, and security communities, including through the OpenSSF's general Slack channel and Open Forum Europe's email list. The survey, which was open from November 20, 2022, through January 8, 2023, aimed to gather attitudes on OSS policy and security from OSS maintainers, developers, and stakeholder communities closer to the problem set than policymakers in government. Despite being open to over two thousand potential respondents, the survey only achieved a sample size of forty-six, limiting the insight into community priorities that it could provide. Nonetheless, there were some noteworthy trends in the responses, and the Atlantic Council and Open Source Policy Network will continue to gather outside perspectives and sentiment trends in this manner.

1. Main respondent affiliation

Government	ICT Vendor	Non-ICT Vendor	Independent Researcher	Academia	Nonprofit organization	Other
2	16	4	3	4	9	8
4.3%	34.8%	8.7%	6.5%	8.7%	19.6%	17.4%

2. Respondent's primary role with respect to OSS (select all that apply):

Maintainer	Contributor	User	None of the above
29	32	34	5
63.0%	69.6%	73.9%	10.9%

3. If you had to pick one party to assume more responsibility than they currently do for security outcomes associated with the use of open-source software, which would it be?

ICT Vendors	All Industry	OSS devs	Foundations/ Nonprofits	Gov	Other
9	20	2	5	8	2
19.6%	43.5%	4.3%	10.9%	17.4%	4.3%

4. Which is the most useful characteristics for assessing the health and well-being of an open-source community, if you had to pick just one?

Project activity	Contributor community	Maintainers	High-activity contributors and maintainers	Community principles	Security expert involvement	Other
7	5	5	12	5	4	8
15.2%	10.9%	10.9%	26.1%	10.9%	8.7%	17.4%

5. Which is the most critical function of an Open-Source Program Office (OSPO) if you had to pick just one?

Public education and awareness	Public-private coordination management	Funding	Licensing + auditing policies	OSS engagement	Other
5	4	14	9	9	5
10.9%	8.7%	30.4%	19.6%	19.6%	10.9%

6. Where do you see the tooling or information gap that might be most harmful to the OSS ecosystem?

Project metadata	Usage data	Vulnerability reporting	Vulnerability info access	Security testing	SBOM generation	Other
1	11	3	2	12	5	12
2%	24%	7%	4%	26%	11%	26%

7. Please sort these methods of external support for, and investment in, open-source projects from most useful to least useful open-source maintainers and developers, in your opinion and relative to each other.

	1-Most useful	2	3	4	5-Least useful
Security testing/assessments	14	14	12	5	1
Bug-bounty programs	1	12	11	11	11
Security info-sharing and procedures	2	17	13	1	13
Incident response support	5	16	9	13	3
Direct funding	25	8	6	6	1

8. Please sort these heuristics for assessing the risk of using a specific OSS package from most useful to lease useful, in your opinion.

	1-Most useful	2	3	4	5	6	7-Least useful
Project popularity	7	11	8	10	2	3	5
Community size and activity	13	13	11	6	1	1	1
Cost of maintenance and usage	3	7	9	7	11	1	8
Fulltime developer count	9	11	10	8	4	2	2
Recent significant vulnerabilities	7	11	12	7	3	6	0
Number of corporate sponsors	4	4	7	8	6	12	5
Number of individual sponsors	2	3	5	5	14	9	8

9. Please sort these methods of external support for, and investment in, open-source projects from most useful to least useful for the security of downstream users.

	1-Most useful	2	3	4	5-Least useful
Security testing/assessments	18	13	10	2	3
Bug-bounty programs	1	12	10	12	11
Security infosharing and procedures	4	15	15	2	10
Incident response support	7	17	8	12	2
Direct funding	22	8	6	6	4

HOW MUCH DO YOU AGREE OR DISAGREE WITH THE FOLLOWING STATEMENTS?

10. A government role in supporting the open-source ecosystem is necessary for its long-term sustainability and success.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
16	14	8	5	3
34.8%	30.4%	17.4%	10.9%	6.5%

11. Government support must include direct financial investment to ensure the open-source ecosystem's long-term sustainability and success.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
14	18	8	4	1
30.4%	39.1%	17.4%	8.7%	2.2%

12. Tell us about your bogeyman – where do you see the most risk across the OSS community? Answers here can reflect either security risks, dangers posed by policy, or other concerns.

- Moving software to memory safe languages and actionable OSS supply chain management are the highest risk issues, IMO.

- Lack of proper project governance, in particular for accepting commits.

- Rogue maintainers who sabotage their own work for whatever reason.

- siloing of information about os production and consumption leading to ineffectual allocation of support/resources.

- lack of coordinated engagement by all relevant stakeholders: the community, foundations and other industry bodies, government and consumers (especially large global ones)

- I fear that the burden (via law/policy) of ensuring secure software will be set unrealistically (zero bugs) and fall (with serious consequences) on individual contributors. This would effectively kill the OSS ecosystem by creating huge disincentives for anyone to be involved.

- The volume of mission critical code that is written in a memory unsafe language is highly alarming - it's so bug-prone and those bugs are often part of an exploit chain.

- lack of security awareness and efforts by OSS developers.

- Tragedy of the commons, and assumption that someone else will do "it".

- Putting too much of the burden on volunteer maintainers. Companies shouldn't try to require too much of the free projects that they are using. Any interventions must come with strong community incentives.

- Increasing and poorly tracked dependency on projects, in some cases individuals, misalignment of funding and resources, treating OSS as a public good (gov investment) is maybe sound, consider tax concepts (really), who benefits more should pay/fund more, cui bono, shouldn't be a complete gov subsidy.

- Transitive dependencies, where users evaluate the parent OSS project, but not all of its dependencies to see if they are well maintained and following best practices.

- Funding. The world is capitalism, and it is not practical for critical open source maintainers to focus on that job full-time without capital.

- NULL

- Users of open source don't understand that in many/most cases that the software isn't supported in the same was commercial software is. Example, I recently say a user ask about when some vulnerabilities that have been published would be addressed in the project. This project is widely used and has critical vulnerabilities in it. The single maintainer's response was "it simply depends on my spare time." Critical security issues in what is likely critical software for some orgs and it will be addressed when someone has some spare time. That's not a formula for highly secure software.

- Education and knowledge gap

- The Jeeper Creeper

- Government attempting to regulate an anti-culture which is based entirely on the foundations of helpfulness, novelty, and innovation. Open source is not industry, it is not corporate, and the ideals of it are often at odds as those using it. It's like volunteer EMTs or Good Samaritans. There should be support and protections for those that do the reasonable right thing without introducing a burden on them.

- Security loopholes should addressed with caution and strict measures.

- comprehensive and aligned and equal support for both upstream creators of open source and downstream consumers is critical

- Risk: death and burnout. We are currently ignoring both in the name of security and that's going to bite us.

- Funding. Governments should require a % of profit - not even revenue, just profit - be invested into their open source stack.

- Trey Herr really worries me. Don't let him near a command line.

- The biggest risk is automation without proper processes and workflows in-place. Automating a process incorrectly is a greater risk than not doing it at all.

- Biggest risk across OSS community is sustainable - having alpha-omega and free security trainings is nice but research has shown most of OSS projects have a single maintainer. How can you expect a single maintainer to maintain his/her project and also spent time on security considerations? We need an open source way to give OSS usesr (especially large enterprise) easy insights into OSS usage so they then can undertake action to support the OSS projects vital/critical to them (have seen people use OSS Review Tookit for this)

- One of the most significant issues is a cultural one. Today, most conversations around open-source software still put too much emphasis on the community aspect and define it as some charity. The solutions are usually related to increasing long-term volunteer contributions from corporations or individuals.However, if the open-source initiatives had the necessary financial resources, like any other businesses, they would already do their best to minimize the risks, hire the needed talents and produce a healthy software solution. Hence, we should recognize the overall economic value of open-source software, see it as a regular business activity in which entrepreneurs contribute to digital public goods, and address investment coordination issues around it.Once the open-source ecosystem receives adequate funding, the competition in the market should sort out the rest.

- Projects fail or are mismanaged due to lack of organizational support.

- Not having an asset list of what actually the enterprise has

- Insider risk or the malicious maintainer - Open source projects can switch hands or be influenced by anyone despite their motivations or backgrounds. This is an incredible difficult security risk to address for OSS.

- Government overreach would be a concern. Standards would be helpful.

- A monopoly on the code hosting services

- security fatigue due to vendors overselling BS, generally the amount of bad security vendors and products

- Lack of direct funding for core nodes, central components in wide use. Lack of practical contributions by ENISA, see e.g. their analysis of Heartbleed in someoneshouldhavedonesomething style, bugbounty programs on a too small scale without larger buy-in of officials, no large scale strategic investment in open source with regards to platform dependencies of the economy, that is, no learnings from the Putin gas disaster, dependencies from China in the hardware sector.

- Security risks. Code bases not checked by real security experts.

- Throwing OSS under geopolitical bus

- Lack of critical thinking and understanding of biaised axioms

- Government/large corporate business users failing to financially support the open source projects they use. Government stepping in and trying to regulate/control a system that does not want or need this. Government depts. trying to be software developers.

- Funding Public, Security

- software patents

- An inability to objectively and discrete measure risk assocaited with different OSS projects.

- It's a fact that very few projects have been undergone independent security review. More funding should go into initiatives that can do that. Furthermore, even "well-supported" projects are prone to vulnerabilities and exploits; so projects need to be consistently evaluated and reviewed based on their risk and usage.

- License changes in existing and widely used open source components and libraries. For example, Akka is changing its license from OSS license to a commercial license. All the other OSS components and libraries depending on Akka need to change Akka to some other library or try to meet the requirements of the new license (which is not always possible).

- Regulation that fails to account for the dynamics of the work project that is open source.

- Most surveys of this ilk have a common top blocker: time available to address this priority with everything else to be done. While there are such time constraints amongst OSS devs and maintainers, the risks are high that security issues won't get addressed in the optimal way.

- Blindly relying on projects without ensuring they have a long-term viability.

- The biggest risk I see is in continuity. If the primary maintainer(s) of a popular project leaves the project for whatever reason (burn-out, interest changes, death, etc.), what can the overall open source community to do help that transition?

Atlantic Council

Board of Directors

[redacted]

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today’s global challenges.

1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org