BROOKINGS

Report

Strengthening digital infrastructure: A policy agenda for free and open source software

Frank Nagle Thursday, May 19, 2022

Editor's Note:

This is a Brookings Center on Regulation and Markets policy brief.

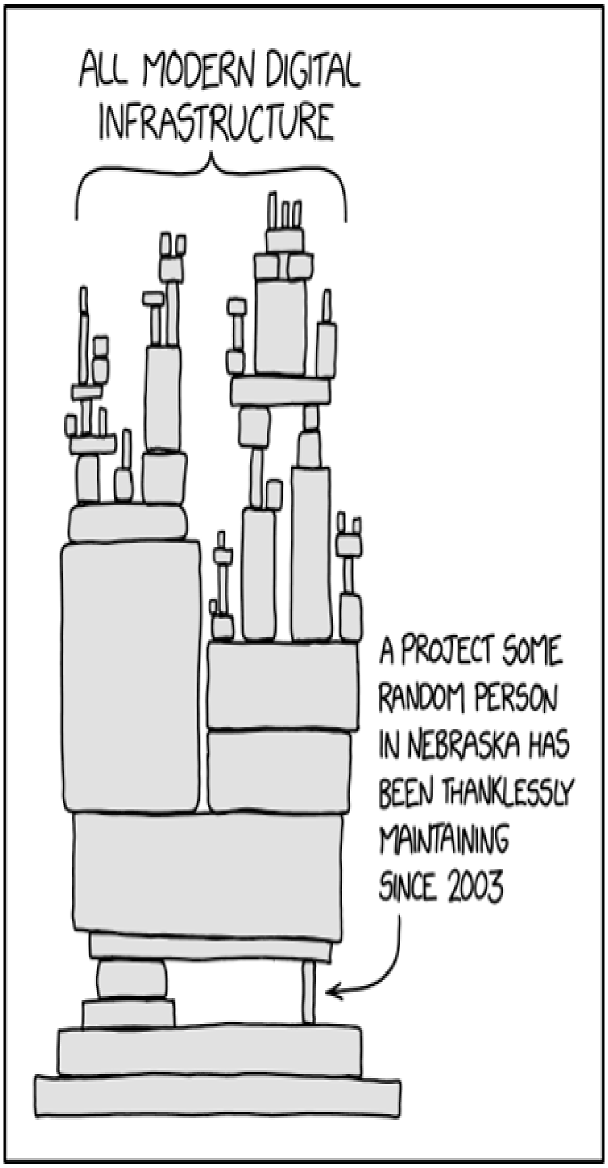
While there is little debate that digital forces are playing an increasingly crucial role in the economy, there is limited understanding of the importance of the digital infrastructure that underlies this role. Much of the discussion around digital infrastructure has focused on broadband availability (which is certainly important), but the role of free and open source software (FOSS or OSS) has gone underappreciated. FOSS—software whose source code is public, is often created by decentralized volunteers, and can be freely used and modified by anyone—has come to play a vital role in the modern economy. It is baked into technology we use every day (cars, phones, websites, etc.), as well as into various aspects of critical infrastructure including our finance and energy systems.

Like physical infrastructure, this digital infrastructure requires regular investment to further enable innovation, commerce, and a flourishing economy. However, also like physical infrastructure, there is a market failure in the private sector that leads to an underinvestment in digital infrastructure. Therefore, there is a clear need for government investment and regulation to ensure the future health, security, and growth of the FOSS ecosystem that has become indispensable to the modern economy.

In this article I lay out policy proposals based on my academic research and that of others, as well as policies that exist in other countries who are ahead of the United States on investing in this critical asset. I first discuss the overall challenge FOSS faces and the limits of existing policy in the U.S. (which are primarily focused on government usage of FOSS, not on investing in the FOSS ecosystem directly). Finally, I present 11 policy proposals separated into four domains of focus: creating an open source program office; measuring and understanding the FOSS ecosystem; enhancing the positive economic impact of FOSS; and securing the FOSS ecosystem. Although there is no silver bullet for guaranteeing the future health and growth of FOSS, these proposals will go a long way towards ensuring FOSS can continue to play its essential role in enabling the modern U.S. economy to grow and flourish.

The challenge

At the highest level, the challenge related to FOSS is that despite its value to the modern economy, its decentralized and free nature leads to both an underappreciation of this value and an underinvestment in its growth and security.


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Source: XKCD, https://xkcd.com/2347/, licensed under Creative Commons Attribution-NonCommercial 2.5 License

On the value side, although it has been estimated that up to 98% of codebases include FOSS, it can be difficult to measure its value. Traditional measures of the value of a product, such as multiplying the number of times a product is used times the price of the product and subtracting input costs, do not work. The price is zero, the labor is volunteered, and measuring the volume of usage is extremely difficult due to the distributed nature of FOSS and the fact that it can be copied and reused freely. Despite these challenges, there have been some recent efforts to value FOSS by myself and others. For example, our early efforts to measure the value of just one piece of FOSS—the widely used Apache web server—found that in 2013, it added up to $12 billion to the U.S. economy, despite not showing up directly in any GDP statistics. More recently, a European

Commission sponsored report found that in 2018, EU companies invested roughly €1 billion into FOSS creation, which resulted in up to a €95 billion benefit for FOSS users in the EU. Similar estimates for the U.S. investment in FOSS were $33 billion in 2019. However, despite these attempts, we have only scratched the surface of truly understanding the value FOSS provides to the economy and modern life. This is even more so the case when considering the value created in the context of digital autonomy, as an increased reliance on FOSS can limit the occurrence of single points of failure where a company or country is beholden to a particular company that provides proprietary software or owns a patent (especially in the context of communications standards, like 5G).

On the investment side, the challenge is twofold. First, despite increasing evidence for a high rate of return to public and private investment in FOSS that can enhance competitiveness and innovation, the U.S. has yet to make a concerted effort to directly invest in it—beyond just supporting its use in federal agencies. The U.S.'s investments in the Global Positioning System (GPS) is an example of the success such investments can have—U.S. investments in GPS, which is made freely available to users, have enabled $1.4 trillion of economic gains for U.S. companies (which the government receives tax revenue on). Likewise, our work on Apache showed that government investments in FOSS can lead to a rate of return of at least 17%, more than double the U.S. government's commonly used baseline of 7% representing a good investment opportunity. Broader analysis in the European Commission report revealed a cost-benefit ratio of roughly 1:4 for FOSS investments by private companies, and my own work on government support of FOSS in France showed a variety of positive outcomes, including as much as an 18% increase in the founding of French IT-related startups and as much as a 14% increase in the number of French workers employed in IT-related jobs. Even for companies, my research has shown that not only does using FOSS lead to productivity gains but investment in FOSS can pay dividends as companies that contribute to FOSS obtain up to 100% more productive value from using FOSS than their free-riding peers.

Second, an underinvestment in FOSS can result in security concerns that have economy-wide consequences. The most recent evidence of this was the 2021 discovery of the Log4Shell vulnerability in the FOSS logging package log4j. Deployed across a vast range of digital applications, the vulnerability was originally introduced in the code in 2013 and exposed tens of millions of devices to a devastating security vulnerability and illustrated the urgent need to improve security in open source software. Jen Easterly, the director of the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) called Log4Shell "the most serious vulnerability I've seen in my decades-long career," and well before most organizations could patch the vulnerability, there were over 800,000 attacks using it in a 72-hour period, including some by Chinese and Iranian government-sponsored actors. Government policy can help identify and address these vulnerabilities in a timelier fashion.

Limits of existing policies

The biggest limit to existing U.S. policies related to FOSS is that they are nearly all focused on the federal government's use of, creation of, and purchasing of technology for its own systems. No policies are targeted at measuring, investing in, or securing the FOSS ecosystem as a whole or in a direct manner. Although my prior research has shown that governmental policies favoring the usage of FOSS in technology procurement can have important positive spillovers to a country (as well as cost savings), this is more of a second-order impact rather than the first-order impact direct investment can have. There are numerous examples of such procurement policies. As early as 2004, agencies of the U.S. federal government started to clarify their stances towards FOSS. However, it was not until the Office of Management and Budget memorandum M-16-21 in 2016 that a clearer pro-FOSS stance was taken. M-16-21 required that all federal agencies should a) make all new custom code for any federal agency available for reuse across all federal agencies, and b) release at least 20 percent of new custom code as FOSS for anyone to use. These efforts were coordinated through the Code.gov website, originally developed under the Office of the Federal Chief Information Officer and now administered by the U.S. General Services Administration (although recently defunded and essentially static). To this day, M-16-21 is the primary guidance on how federal agencies should approach FOSS and is the primary authority cited within numerous agencies related to their FOSS stance (e.g., Department of Commerce and Department of Defense). These efforts were expanded upon with the May

2021 White House Executive Order 14028, which included a section requiring all federal government software purchases to include a software bill of materials (SBOM) that clearly stated what other software (including FOSS) was built into the purchased software.

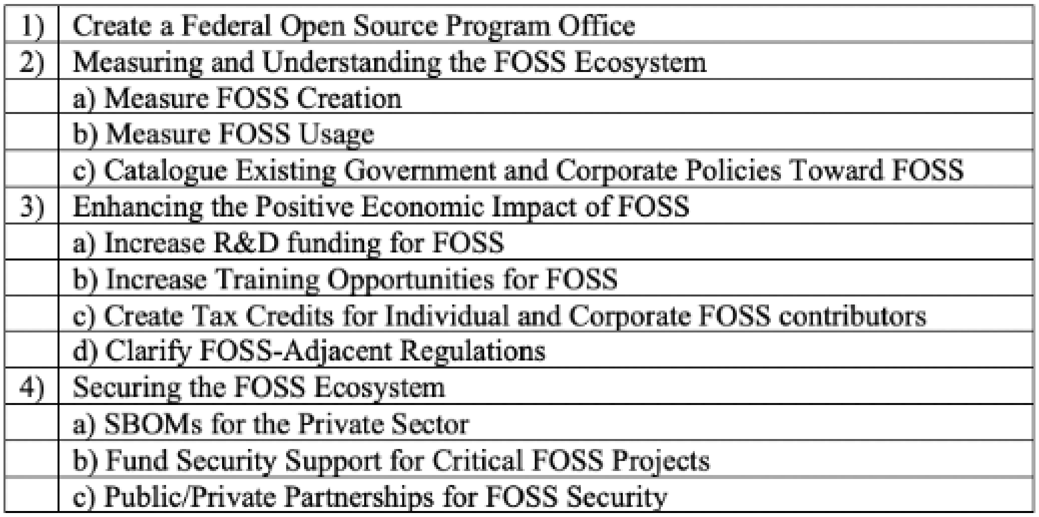
Beyond M-16-21, a handful of other governmental efforts have been proposed but not passed. For example, the House version of the 2022 National Defense Authorization Act included funding for a FOSS security center within DHS, but the funding did not make it into the final bill. At the state level, New York has introduced a bill to give a tax credit for expenses related to developing FOSS in every legislative session since 2009, but the bill has never gotten out of committee. Even the much-praised bipartisan infrastructure package passed in late 2021 focused its digital infrastructure investments nearly exclusively on broadband availability and did not address investments in FOSS.

Most recently, in January 2022, in response to the aforementioned Log4Shell vulnerability, the White House National Security Council (NSC) held a meeting with companies like Google and Microsoft; open-source organizations including the Linux Foundation, the Apache Software Foundation, and the Open Source Security Foundation (OpenSSF); and numerous federal agencies and departments. The meeting focused on preventing, finding, and shortening response time to FOSS vulnerabilities and discussed various potential public-private partnerships. Although there were no concrete pledges from the meeting, the intent was to start a discussion, identify possible paths forward, and commit to future meetings that would yield specific commitments by the various stakeholders. In May of 2022, the first follow-up meeting was held and it identified 10 areas of focus to improve OSS security and provided specific plans of action and a call for $150 million in funding over two years. The intent was for this funding to come from private companies, not the government, and some large tech companies have already committed $30 million to assist in the effort.

Policy recommendations for supporting FOSS as critical digital infrastructure

Given the lack of federal policies directly supporting the FOSS ecosystem, I lay out 11 policy proposals that can help to support the FOSS ecosystem in critical ways (overviewed in Table 1). These policies are grouped into four domains. The first domain is to create a new office to oversee all FOSS related activity within the federal government. The second domain focuses on measuring and understanding the FOSS ecosystem, which is necessary given the distributed nature of FOSS, and the lack of a clear understanding of how pervasive it is in the modern economy. The third domain considers avenues for investing in FOSS to help enhance the economic competitiveness of the U.S. The fourth domain focuses on methods for securing existing and future FOSS to reduce the likelihood of some of the issues mentioned above. Some of the policy recommendations build upon the European Commission report mentioned above, for which I was an outside advisor, but consider how (and where) they could be applied in the U.S. Further, although all of these recommendations are focused on FOSS, they can be thought of to include free and open source hardware as well, which is a smaller space than FOSS but is rapidly growing and is increasingly important to the economy.

Table 1: Recommendations for Strengthening Digital Infrastructure



1)	Create a Federal Open Source Program Office
2)	Measuring and Understanding the FOSS Ecosystem
	a) Measure FOSS Creation
	b) Measure FOSS Usage
	c) Catalogue Existing Government and Corporate Policies Toward FOSS
3)	Enhancing the Positive Economic Impact of FOSS
	a) Increase R&D funding for FOSS
	b) Increase Training Opportunities for FOSS
	c) Create Tax Credits for Individual and Corporate FOSS contributors
	d) Clarify FOSS-Adjacent Regulations
4)	Securing the FOSS Ecosystem
	a) SBOMs for the Private Sector
	b) Fund Security Support for Critical FOSS Projects
	c) Public/Private Partnerships for FOSS Security

1. Create a federal Open Source Program Office

An open source program office (OSPO) is an entity that seeks to centralize an organization's FOSS efforts—usage of, contribution to, policies towards, etc. While some federal agencies and departments have setup their own OSPOs, there is no central federal body designed to manage the government's overall approach to FOSS. Code.gov is the closest existing entity to this; however, its mandate is much narrower than that of a true OSPO. In addition to coordinating the use of FOSS by government entities (as Code.gov currently does), the OSPO would also coordinate federal policies related to FOSS, like those laid out in the recommendations in this document. The lack of such an office is likely why the federal government's efforts related to FOSS have been highly disjointed to this point. The OSPO could be located within the White House Office of Science and Technology Policy (OSTP), within the office of the U.S. Chief Technology Officer (CTO). OSTP is tasked with leading government efforts to implement technology policies, and thus is in a good position to take ownership of this effort. This office could coordinate with existing OSPOs in federal agencies and could help stand up OSPOs in agencies that do not yet have them. In this capacity, it could oversee the implementation of the remainder of the recommendations here, in conjunction with the various additional government bodies identified below. Further, it could take over the Code.gov efforts that have recently been defunded. Finally, the OSPO could manage international collaboration and coordination with other countries to amplify mutual interests and share in the benefits.

2. Measuring and understanding the FOSS ecosystem

To properly measure and understand the FOSS ecosystem in the U.S., more data is required in three specific areas: creation, usage, and policies. There are parallels in the complexities of aggregating such data to the drawing of U.S. broadband maps that have been seen as essential to influencing and informing the rollout of broadband internet connections in the U.S., another aspect of digital infrastructure. The data are messy and reside with numerous separate entities, but once aggregated in a clear and complete manner, can provide deep insights into how to best go about addressing the challenges discussed above.

a) Measure FOSS creation

Although measuring the creation of FOSS is far easier than measuring its usage (addressed below), it is still a complicated task. FOSS generally resides in repositories and foundries like GitHub, GitLab, and Bitbucket. However, it is sometimes maintained on individual project pages, which can make measuring the full extent of FOSS difficult. Additionally, many contributor profiles on such repositories have no information other than a username. Thus, gaining insights into the people contributing to FOSS is not trivial, making a better understanding of the low levels of diversity in FOSS contribution difficult. Further, it is not always possible to know if a contributor to FOSS is doing so at the behest of their employer as part of their paid employment, an increasingly common occurrence. Thus, measuring FOSS creation (and creators) will require a multipronged approach. First, OSTP and the U.S. CTO should attempt to aggregate data from the disparate sources of FOSS and regularly update it to track what projects exist, what their function is, who their contributors are, and how active they are in maintaining projects and fixing known issues. Second, to better measure corporate involvement in FOSS creation, questions should be added to the U.S. Census Bureau's Management and Organizational Practices Survey (MOPS). This survey is run every five years as an addendum to the Annual Survey of Manufacturers and aims to "better understand current and evolving management and organizational practices and to assist in identifying determinants of establishment and productivity growth." Previous questions about technology usage have been added to the MOPS and revealed important insights about how firms use technology (e.g., predictive analytics and artificial intelligence) to enhance their productivity.

b) Measure FOSS usage

For the variety of reasons mentioned above, accurately measuring FOSS usage is extremely difficult. However, a number of efforts, including our own, have sought to shine light on this multi-faceted challenge. While these efforts have chipped away at the problem, an effort sponsored by the federal government is more likely to lead to a wider understanding of FOSS usage in the U.S. Again, a multipronged approach is optimal. First, using aggregated data from key stakeholders including cloud providers, software composition analysis companies, FOSS package managers, and FOSS repositories and foundries that have insight into FOSS usage, OSTP and the U.S. CTO can create statistics on what FOSS packages are most widely used. It would be critical to conduct this analysis at all levels of the software stack, including operating systems, application libraries, cloud containers, and end user applications. Second, the Census Bureau can add additional questions to the MOPS to gauge open source usage by companies—both those who make software and those who only use it.

c) Catalogue existing government and corporate policies toward FOSS

Understanding government and corporate policies toward FOSS allows for better guidance on how the details of the policy proposals below should be crafted for optimal effectiveness. Many other countries are ahead of the U.S. in FOSS-related policies and aggregating and studying them can provide additional guidance into how U.S. FOSS policies should be crafted. Some surveys of governmental policies exist but have not been updated since 2010. Such an effort could be conducted via OSTP and the U.S. CTO. Additionally, our work has shown that companies have a wide range of policies towards FOSS, many of which their employees do not fully understand. Additional questions can be added to the Census MOPS to understand the range of policies companies have to better allow research to provide guidance for optimal business policies. This can include policies about using and contributing to FOSS, as well as whether or not the company has an OSPO to manage such efforts.

3. Enhancing the positive economic impact of FOSS

Not only does FOSS create economic value directly (as discussed above), but it also allows businesses of all types to grow more quickly than if it didn't exist. This is particularly the case in the context of small and medium enterprises (SMEs) that are credit constrained and would not be able to build the tools that FOSS provides from scratch. Thus, at a national level, investments in FOSS can enhance national competitiveness and enable greater levels of R&D and innovation in all sectors. Therefore, it behooves the U.S. to support the FOSS ecosystem directly to augment its positive economic impact. This can be achieved through a variety of policy measures including increasing R&D funding for FOSS, lowering the costs of FOSS participation for SMEs, increasing training opportunities, creating tax credits for individual and corporate FOSS contributors, and clarifying FOSS-adjacent regulations.

a) Increase R&D funding for FOSS

Currently, there is no federal funding for R&D related to FOSS despite growing evidence that this can lead to a great number of outcomes whose benefits outweigh the cost of investment. Therefore, the federal government should build upon existing programs from the private sector to enhance FOSS related R&D. This can come in the form of grants for researchers studying FOSS and FOSS communities themselves. The most logical places to host these grants are through the National Science Foundation, or through the Department of Commerce's National Institute of Standards and Technology (NIST), both of which manage grants related to technology R&D. Further, since an outsized amount of FOSS is created by SMEs, specific grants targeted at them can also be offered through the Small Business Association (SBA), which already offers grants and loans for SMEs doing work in particular spaces.

b) Increase training opportunities for FOSS

The federal government should support increased training opportunities through both traditional academic environments and continuous learning settings. This would include grant programs through the Department of Education (DOE) to add FOSS skills to existing computer science curriculums at all educational levels as well as enabling individual grants to sponsor pursuit of continuing education programs targeted at employers in relevant industries. Other targeted grants are already managed by DOE and FOSS-related grants could be added into the existing system. Further, offering training about FOSS to SMEs would likely go a long way towards this end. Such training could be offered through existing efforts targeted at SMEs, like the SBA's Learning Platform.

c) Create tax credits for individual and corporate FOSS contributors

Tax policy has long been used to incentivize businesses and individuals to increase a particular behavior that has social benefits. Therefore, this is a logical tool to use to increase FOSS creation in the U.S. For individuals, the New York proposal mentioned above to grant a tax credit for FOSS development expenses could be easily applied to a national setting. However, a federal FOSS tax credit could go beyond only crediting direct expenses related to FOSS (e.g., purchasing cloud computing resources) to also include uncompensated (e.g., by an employer) time spent on contributing to FOSS. Although donations of volunteered time are not usually allowed as a write-off, the fact that the result of this time is software, which can be written off as a donation, should allow for a small addition to the tax-code that would not open the door to all volunteer time being allowed as a write-off.

For companies, a simple addition and clarification to the existing R&D tax credit would allow companies to reduce their tax burden by contributing to FOSS. Currently, companies are allowed to apply investments into internal software development towards the credit. However, there is a lack of clarity around whether or not investments in creating FOSS are eligible for the R&D tax credit. Therefore, clarity on the topic that allows for such investments to be eligible for the R&D tax credit would encourage companies to invest more in FOSS. Tax breaks would be particularly useful for lowering the costs of participation for SMEs.

d) Clarify FOSS-adjacent regulations

There are numerous existing regulations in the U.S. that can be seen as FOSS-adjacent in that they may apply to FOSS, but exactly how they apply to FOSS is not clear. For example, there are a wide array of FOSS licenses, and each of them treats aspects of FOSS usage differently (e.g., whether the FOSS package can be used in software that is then sold to customers). In particular, liability concerns associated with different licenses are often misunderstood. In the absence of trial law to clarify such issues, insights from regulatory bodies and the Department of Justice (DOJ) could be useful. Further, FOSS is increasingly being built upon for technology standards. They are often bundled with other patented technologies thus creating a valuable standard that is subject to licensing fees payable to the patent holders. However, despite FOSS creating value for the standard, that value is being captured by patent holders. Thus, regulations related to the interplay between FOSS and patents in standards requires clarifications by key stakeholders like NIST. Finally, as corporations increasingly contribute to FOSS, antitrust and collusion concerns may arise.

For example, if two competitors are contributing to the same FOSS project, are there anti-competitive concerns that the two companies are exposed to? The answer in some situations may be yes, but current regulations require clarification from regulatory agencies like the Federal Trade Commission and the Antitrust Division of the DOJ. In my broad research agenda, I argue that in many settings, it may be optimal—for companies and consumers—to allow competitors to "collaborate on the core and compete on the edges," but there is a lack of consensus on where the line between such collaboration and anticompetitive behavior lies.

4. Securing the FOSS ecosystem

The fourth, but equally important, domain of FOSS policy recommendations is focused on securing existing and future FOSS, to ensure it can continue to play an increasingly critical role in the economy. As mentioned above, as FOSS is more deeply integrated into everyday life, security issues like the Log4Shell vulnerability can pose a bigger risk to the continued smooth functioning of the economy built on top of FOSS. However, unlike well-structured (and well-funded) companies developing proprietary software, security in FOSS is either an afterthought, or not thought of at all. Indeed, our research has shown that most FOSS contributors want to focus on adding new features, rather than performing security audits or addressing vulnerabilities. Therefore, in addition to, and building upon, the policy recommendations above are three recommendations directly related to security. Importantly, security efforts would be a particularly ripe area for international collaboration since enhanced security is beneficial to all FOSS users.

a) SBOMS for the private sector

Currently, SBOMs (software bills of materials, mentioned above) are only required for software purchased by the federal government. However, there could be a great deal of benefit for also requiring such digital ingredient lists for private sector purchases of software as well. One of the problems with vulnerabilities like Log4Shell is that many companies (and individuals) were uncertain if they were vulnerable to the issue because they did not know if the vulnerable log4j component was included in software and Internet of Things devices they had purchased. For example, although it was widely understood that production software used at companies including Apple, Google, Amazon, Twitter, and Tesla included vulnerable versions of log4j, their customers were in the dark due to a lack of an accurate SBOM. With a clearer view into the software baked into the software they have purchased, customers and consumers would be able to immediately know if they were vulnerable to such security issues. Importantly, such insight would be particularly valuable in the context of the "right to repair," which was promoted as part of last year's Executive Order on competition, such that companies would be able to upgrade to a patched version of a vulnerable software component.

Although this would be a far-reaching mandate for private companies, precedence for such regulation can be found in the efforts of the Food and Drug Administration requiring an ingredient list on most food labels. Although software may not be as fundamental to everyday life as food, its increasingly important role warrants the increased transparency SBOMs would provide. Such a regulation could be managed through existing offices in the Department of Commerce's National Telecommunications and Information Administration or the Federal Communications Commission.

b) Fund security support for critical FOSS projects

Given the nature of FOSS as a public good (like roads and bridges), it only makes sense for the U.S. government to invest in its security to ensure the digital infrastructure of the modern economy is stable, enabling businesses and individuals to continue building upon it as they have done for decades. In particular, investments in security audits (and providing resources to fix issues identified in such audits), educational and mentoring resources for smaller FOSS projects, and standardized measurement and publication of security practices would likely yield high returns on investment. The results of the above policies related to measuring and understanding the FOSS ecosystem could be used to prioritize and target such investments to increase their immediate impact. Further, efforts related to Code.gov could lead to a better understanding of the critical FOSS the federal government relies upon and could also be used for prioritization of investments. Importantly, these efforts would not be starting from scratch as the OpenSSF and others have laid the ground for these actions through their auditing, educational, and badging programs.

c) Public-private partnerships for FOSS Security

As mentioned above, in response to the Log4Shell vulnerability, the White House NSC sponsored a multi-party meeting including representatives from government, the private sector, and nonprofit FOSS organizations. Although it is too early to tell what will come of this effort, it was a critical first step to adding a layer of coordination to a notoriously decentralized problem. Although there have been public-private partnerships related to cybersecurity before (notably the Federal Bureau of Investigation Infragard and the DHS CISA Critical Infrastructure Sector Partnerships), these tend to be focused on information sharing. Efforts building upon the NSC meeting need to include a focus on collective action and investment in securing FOSS by key stakeholders across sectors.

Conclusion

Although these proposals are not a panacea for the challenges facing the FOSS ecosystem, they are critical steps to ensuring the health and growth of an indispensable building block of the modern economy. Much as roads and bridges are only useful if there is somewhere worth traveling to, future discussions about digital infrastructure must go beyond only considering broadband availability and must include a focus on the FOSS that underlies the digital economy we rely upon every day. By measuring and understanding the FOSS ecosystem, enhancing its positive economic impact, and securing it with the policy recommendations above, we can help pave the way for a U.S. economy that is more innovative, more competitive, and more resilient than ever before.

The author's research is partially funded by The Linux Foundation. The author did not receive financial support from any firm or person for this article or, other than the aforementioned, from any firm or person with a financial or political interest in this article. They are currently not an officer, director, or board member of any organization with an interest in this article.

Enter Email Enter Email Subscribe

No thanks, just download the file.