TRAGEDY OF THE DIGITAL COMMONS[*]

CHINMAYI SHARMA[**]

Google, iPhones, the national power grid, surgical operating rooms, baby monitors, surveillance technology, and wastewater management systems all run on open-source software. Open-source software, or software that is free and publicly available, powers our day-to-day lives. As a resource, it defies economic logic; it is built by developers, many of whom are volunteers, who build projects with the altruistic intention of donating them to the digital commons. Developers use it because it saves time and money and promotes innovation. Its benefits have led to its ubiquity and indispensability. Today, over ninety-seven percent of all software uses open source. Without it, our critical infrastructure would crumble. The risk of that happening is more real than ever.

In December 2021, the Log4Shell vulnerability demonstrated that the issue of open-source security can no longer be ignored. One vulnerability found in a game of Minecraft threatened to take down systems worldwide—from the Belgian government to Google. The scope of damage is unmatched; with open source, a vulnerability in one product can be used against every other entity that uses the same code. Open source's benefits are also its burden. No one wants to pay for a resource that has an unlimited supply, available for free. Open source is not, however, truly unlimited. The open-source community—the individuals, nonprofits, and companies actively contributing to its production and

[**] Scholar in Residence at the Robert Strauss Center for International Security and Law and Lecturer at the University of Texas School of Law. I would like to thank Dean Robert Chesney, Adam Klein, Alan Rozenshtein, Michael Dolan, Karen Copenhaver, Charles Barzun, Orin Kerr, Peter Swire, Josh Goldfoot, Ashwin Ramaswami, Brett Frischmann, Bruce Schneier, Allan Friedman, Jacques Chester, James Howison, Chris Hughes, members of the Cybersecurity Law and Policy Scholars conference, members of the Nebraska Governance and Technology Center workshop, and James Tomberlin for encouragement, advice, and thorough feedback on earlier drafts. This Article would not have been possible without the insight provided by members of the Linux Foundation, Apache Foundation, OSTIF, OpenSSF, OTF, Google, Microsoft, Chainguard, GitHub, GitLab, Global Cyber Alliance, and other open-source community members over the course of numerous interviews. In particular, I want to thank Trey Herr, Frank Nagle, John Speed Meyers, CRob, Brian Behlendorf, David Wheeler, Jessica Wilkerson, Daniel Kahn Gillmor, Ari Schwartz, Melissa Hathaway, Amir Montazery, Madison Oliver, Tod Bearsley, Steve Weber, Justin Cappos, Bryan Nunez, Laurent Simon, William Bartholomew, Sean Brooks, Leslie Daigle, Brendan O'Leary, Jonathan Meadows, Ravi Nayyar, and Manoj Prasad. I greatly appreciate the work Marshall Newman and the *North Carolina Law Review* editorial team did to take my Article across the finish line. And the largest thanks goes to Audrey Kim and Alex Rigby for excellent research assistance without which this Article would not exist.

maintenance—is buckling under the weight of supporting over three-fourths of the world's code. Rather than share the load, many of its primary beneficiaries, companies that build proprietary software, add to it. By failing to take basic precautionary measures in using open-source code, they make its exploitation nearly inevitable—when it happens, they free ride on the already overwhelmed community to fix it. This doom cycle leaves everyone worse off because it leaves our critical infrastructure dangerously vulnerable.

Since it began, open source has worked behind the scenes to make society better. Today, its struggles are going unnoticed and unaddressed. The vanguard of public and private entities already supporting open source cannot carry the burden alone—the rest of open source's beneficiaries must also be conscripted. So far, government interventions have been lacking. Secure open source requires much more. To start, it is time we treated open source as the critical infrastructure that it is.

INTRODUCTION 1131
I. WHAT IS OPEN SOURCE AND WHY DOES IT MATTER? 1138
A. *Open Source's Differences from Closed-Source Code*.............. 1138
1. Writing and Using Open-Source Code.................... 1138
a. Open Sourcing Code.. 1139
b. The Value of Using Open Source............................ 1140
c. The Ability To Crowdsource Project Support............ 1142
d. The (Alleged) Pitfalls of Openness........................... 1145
2. The Community Building Open Source 1148
a. Open Source's Developers...................................... 1148
b. Open Source's Support Structures........................... 1152
c. Open Source's Weak Link...................................... 1158
3. Licenses Governing Open Source 1164
B. *Consequences of Open Source's Unique Structure*.................. 1166
1. Open Source Is Everywhere 1166
2. Open Source Has Become Critical Infrastructure 1167
3. Open Source's Security Issue Is a Critical Infrastructure Security Issue...1172
II. OPEN SOURCE'S SECURITY PROBLEM DERIVES FROM ITS PUBLIC GOOD FEATURES 1173
A. *Open Source Is an (Impure) Public Good*............................ 1173
1. Characteristics of a Public Good 1174
2. Open Source as a Public Good..................................1176
a. Non-Excludable 1176
b. Somewhat Rivalrous 1176

B. *Open Source's Market Failures* 1178
1. Free Riders 1178
2. Cost of Externalities Fall on Public 1182
3. Asymmetric Information 1185
C. *Consequences of Open Source's Market Failures* 1188
1. Tragedy of the Commons 1188
2. Unaccountable Least-Cost Avoider 1190
III. GOVERNMENT'S ROLE IN A COORDINATED, COMPREHENSIVE RESPONSE 1192
A. *Coordination Required To Solve Market Failures* 1192
B. *Interventions to Date Have Been Lacking* 1193
1. Voluntary Efforts Are Insufficient 1193
2. Government Interventions Are Piecemeal 1197
a. Limited Scope 1197
b. Limited Enforceability 1203
C. *Tools for a More Effective Response to Open-Source Security* 1205
1. Designate Open Source as Critical Infrastructure 1205
2. Additional Roles for Government To Secure Open Source 1209
a. Government as a Coordinator 1209
i. Information Gathering 1209
ii. Resource Allocation 1212
iii. Information Sharing 1213
b. Government as a Standards Body 1216
c. Government as a Consumer 1217
d. Government as a Supplier 1218
i. Resource Donor 1218
ii. Open-Source Contributor 1221
iii. Security-Services Provider 1222
e. Government as an Enforcer 1224
CONCLUSION 1228

INTRODUCTION

On December 9, 2021, holidays internationally were disrupted when a Chinese security researcher sounded the alarm about a vulnerability—an exploitable code defect—in Log4j, a popular open-source library.[1] Hackers immediately weaponized it.

The United States alone was hit with ten million attempted exploits *per hour*, with attacks specifically targeting critical infrastructure sectors.[2] By some estimates, one in ten digital assets were impacted; this means phones, laptops, smart fridges, baby monitors, pacemakers, cars, and security systems.[3] Even the best paid, most qualified security teams struggled to keep up. Companies like Apple, Amazon, Cloudflare, IBM, Microsoft, and Twitter began experiencing a barrage of attacks and many had no choice but to shut down systems until the vulnerability could be resolved.[4] The Belgian[5] and Canadian[6] governments had to do the same. Internationally, estimates suggest nearly *half* of global corporate networks experienced a successful exploit in the first five days following the vulnerability's discovery.[7]

The vulnerability, later named Log4Shell, became a matter of national security. Researchers found that Chinese hackers linked to the Chinese

[1] John Graham-Cumming, *Inside the Log4j2 Vulnerability (CVE-2021-44228)*, CLOUDFLARE BLOG (Dec. 10, 2021), https://blog.cloudflare.com/inside-the-log4j2-vulnerability-cve-2021-44228/ [https://perma.cc/4PPC-86VS]; *see also CVE-2021-44228*, CVE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228 [https://perma.cc/2VPX-VNF3] (describing the Log4j2 attack).

[2] David Uberti, James Rundle & Catherine Stupp, *The Log4j Vulnerability: Millions of Attempts Made Per Hour To Exploit Software Flaw*, WALL ST. J. (Dec. 21, 2021, 12:15 PM), https://www.wsj.com/articles/what-is-the-log4j-vulnerability-11639446180 [https://perma.cc/7JNJ-HTLG (dark archive)].

[3] *See* Amit Yoran, *One in 10 Assets Assessed Are Vulnerable to Log4Shell*, TENABLE (Dec. 22, 2021), https://www.tenable.com/blog/one-in-10-assets-assessed-are-vulnerable-to-log4shell [https://perma.cc/TUK2-7MVD] ("Of the assets that have been assessed, Log4Shell has been found in approximately 10% of them, including a wide range of servers, web applications, containers and IoT devices.").

[4] *See* Uberti et al., *supra* note 2 (discussing the impact of the Log4j vulnerabilities on technology suppliers).

[5] *Id.*

[6] Pierluigi Paganini, *Quebec Shuts Down Thousands of Sites as Disclosure of the Log4Shell Flaw*, SEC. AFFS. (Dec. 12, 2021), https://securityaffairs.co/wordpress/125556/hacking/quebec-shut-down-sites-log4shell.html [https://perma.cc/7GPD-38EE].

[7] Danny Palmer, *Log4j Flaw: Nearly Half of the Corporate Networks Have Been Targeted by Attackers Trying To Use This Vulnerability*, ZDNET (Dec. 14, 2021), https://www.zdnet.com/article/log4j-flaw-nearly-half-of-corporate-networks-have-been-targeted-by-attackers-trying-to-use-this-vulnerability/ [https://perma.cc/DX6F-PE4L]; *see also* Frank Nagle, *Strengthening Digital Infrastructure: A Policy Agenda for Free and Open Source Software*, BROOKINGS INST. (May 19, 2022), https://www.brookings.edu/research/strengthening-digital-infrastructure-a-policy-agenda-for-free-and-open-source-software/ [https://perma.cc/2ZBQ-ZNB4] [hereinafter Nagle, *Strengthening Digital Infrastructure*] ("[B]efore most organizations could patch the [Log4Shell] vulnerability, there were over 800,000 attacks using it in a 72-hour period, including some by Chinese and Iranian government-sponsored actors.").

government used Log4Shell to exploit several U.S. state governments.[8] The People's Republic of China, in addition to Iran, North Korea, and Turkey, is suspected to have exploited the vulnerability in national systems.[9] It is no surprise that the Cybersecurity and Infrastructure Security Agency ("CISA") Director Jen Easterly called the vulnerability, which had a Common Vulnerability Scoring System Calculator severity score of ten out of ten,[10] "one of the most serious that I've seen in my entire career, if not the most serious."[11]

At the root of the devastation was a vulnerable open-source library. Log4j, a Java-based logging library, is distributed for free and maintained by *volunteers*.[12] Still, it has been downloaded millions of times and is among the most widely used software packages today. Though the Log4Shell vulnerability was first disclosed publicly in December 2021, it has existed since 2013.[13] That means systems were compromised and Log4Shell's vulnerability was likely exploited before anyone knew to worry.[14]

Log4Shell is but one example in a massive ecosystem. Open-source software—free, publicly available code—is ubiquitous.[15] An April 2022 industry study found that ninety-seven percent of the 2,409 codebases analyzed across

[8] Joseph Marks, *Chinese Hackers Breached Six State Governments, Researchers Say*, WASH. POST (Mar. 8, 2022, 10:02 AM), https://www.washingtonpost.com/politics/2022/03/08/chinese-hackers-breached-six-state-governments-researchers-say/ [https://perma.cc/ES6B-XNH2 (dark archive)] ("The hacking group cracked into the states' computer systems during the past 13 months, stealing an untold amount of data, the cybersecurity firm Mandiant found. In some cases, the hackers used a devastating and widespread vulnerability dubbed log4j, according to the report out this morning.").

[9] Sean Lyngaas, *Microsoft Warns China, Iran, North Korea and Turkey Are Exploiting Recently Revealed Software Vulnerability*, CNN (Dec. 15, 2021, 10:56 AM), https://www.cnn.com/2021/12/15/politics/microsoft-china-iran-log4j/index.html [https://perma.cc/N3YG-DTNL]; Edward Graham, *Iranian Hackers Compromised a Federal Agency's Network, CISA and FBI Say*, NEXTGOV (Nov. 16, 2022), https://www.nextgov.com/cybersecurity/2022/11/iranian-hackers-compromised-federal-agencys-network-cisa-and-fbi-say/379832/ [https://perma.cc/R25X-RU5P].

[10] *CVE-2021-44228 Detail*, NAT'L VULNERABILITY DATABASE, https://nvd.nist.gov/vuln/detail/CVE-2021-44228 [https://perma.cc/2LRX-9GQN] (last modified Dec. 9, 2022).

[11] Tim Starks, *CISA Warns 'Most Serious' Log4j Vulnerability Likely To Affect Hundreds of Millions of Devices*, CYBERSCOOP (Dec. 13, 2021), https://www.cyberscoop.com/log4j-cisa-easterly-most-serious/ [https://perma.cc/R67J-2RT6].

[12] *See* David Uberti, *Global Fight Against Log4j Vulnerability Relies on Apache Volunteers*, WALL ST. J. (Dec. 15, 2021, 5:30 AM), https://www.wsj.com/articles/global-fight-against-log4j-vulnerability-relies-on-apache-volunteers-11639564206?mod=article_inline [https://perma.cc/R6MP-SRBZ (dark archive)]. These volunteers are professional developers. *Id.*

[13] Graham-Cumming, *supra* note 1.

[14] Jonathan Greig, *Second Log4j Vulnerability Discovered, Patch Already Released*, ZDNET (Dec. 14, 2021), https://www.zdnet.com/article/second-log4j-vulnerability-found-apache-log4j-2-16-0-released/ [https://perma.cc/ED27-LE5K].

[15] *See infra* Section I.A (discussing difference between closed-source code and open-source code).

seventeen industries contains some amount of open source.[16] Further, seventy-eight percent of the *lines of code* reviewed were open source[17]—underscoring the prevalence of open-source software in the digital economy. Moreover, more than our social media relies on open source; the 2022 study reported that more than half the critical infrastructure codebases analyzed depends on open source.[18] This means an open-source vulnerability like Log4Shell threatens to take down society's most important systems. When the code is everywhere, a single vulnerability can be used to exploit a whole network of entities that use the same code but are otherwise entirely unrelated and largely unable to coordinate a defense.[19] Hackers recognize this potential for cascading destruction—attacks on open-source software vendors saw a 650% increase over just one year.[20]

Open source is not the problem.[21] In fact, it confers countless benefits, from cost savings to innovation.[22] Far from inherently insecure, it is often *more secure* than closed-source[23] code because the entire community can look for bugs

[16] SYNOPSYS, 2022 OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT 4–10 (2022) [hereinafter 2022 SYNOPSYS REPORT], https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2022.pdf [https://perma.cc/4FVM-RUNT].

[17] *Id.* at 6.

[18] *See id.* at 8, 12 (reporting on the percentages of codebases with open-source origins).

[19] *See* Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 ("[B]efore most organizations could patch the [Log4Shell] vulnerability, there were over 800,000 attacks using it in a 72-hour period, including some by Chinese and Iranian government-sponsored actors.").

[20] SONATYPE, 2021 STATE OF THE SOFTWARE SUPPLY CHAIN REPORT 4 (2021) [hereinafter 2021 SONATYPE REPORT], https://www.sonatype.com/hubfs/Q3%202021-State%20of%20the%20Software%20Supply%20Chain-Report/SSSC-Report-2021_0913_PM_2.pdf?hsLang=en-us [https://perma.cc/H3AR-KQJN].

[21] *See* STEPHEN HENDRICK & MARTIN MCKEAY, THE LINUX FOUNDATION & SNYK, ADDRESSING CYBERSECURITY CHALLENGES IN OPEN SOURCE SOFTWARE 19 (2022), https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/LF%20Research/Addressing%20Cybersecurity%20Challenges%20in%20Open%20Source%20Software%20-%20Report.pdfhttps [https://perma.cc/3GP6-PWBU] (finding that over half of all bugs and "vulnerabilities" found were in software developed in-house as opposed to "third-party code," such as an open-source component); *see also* SYNOPSYS, 2017 COVERITY SCAN REPORT 5 (2017), https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/SCAN-Report-2017.pdf [https://perma.cc/VUS2-45EP] (finding that for many popular open-source projects, the quality of security was higher than the industry average).

[22] *See infra* Section I.A.1.b (outlining the positive efficiencies and effects of open-source software).

[23] Closed-source code is often referred to as proprietary or commercial software, though each term can be used slightly differently. Closed-source code means software whose source code is not publicly available; the owner of the software restricts open access to the source code. *See Proprietary Software*, GARTNER, https://www.gartner.com/en/information-technology/glossary/proprietary-software [https://perma.cc/D3XQ-JFQK]. Proprietary code refers to code whose owner retains certain traditional property rights, such as the right to exclude users from viewing, modifying, using, or sharing the code. *See id.* Commercial software refers to code that is produced for sale or supports commercial

and respond to an attack.[24] However, for this advantage to be realized, enough people must actually be looking. This is the problem: because open source is distributed for free, it is being overused and underfunded. Other countries recognize this. Germany wants to treat open-source software as a public good and launched a sovereign tech fund to support open-source projects "just as much as bridges and roads."[25] The United Kingdom launched a two-month-long initiative focusing exclusively on the role of government in securing critical infrastructure built on open-source software and the need to support long-term maintenance.[26] The European Union is exploring "opportunities for dedicated support services for open-source solutions that [it] consider[s] critical"[27] and has gone so far as to commission a report assessing the open source's substantial economic impact and develop a formal three-year holistic open-source strategy.[28]

purposes. *Commercial Software*, TECHOPEDIA, https://www.techopedia.com/definition/4245/commercial-software [https://perma.cc/C2ZA-TBGY]. Almost all commercial software is proprietary software because it retains the right to exclude users by withholding the source code and often imposing a fee. Proprietary code encompasses code developed or used by the public, academic, and nonprofit sectors as well—code that does not serve commercial purposes but is not made open source. However, proprietary code can, and almost always does, contain open-source components. The fact that the software is made exclusionary after the closed-source and open-source components are integrated does not alter the fact that some of its components remain tied to the terms of their open-source licenses. Therefore, for the purposes of this Article, I will contrast open-source code to closed-source code, because the goal of the Article is to highlight the different incentives that govern code that is decidedly exclusionary versus code that is built or acquired as open-source code.

[24] Peter P. Swire,*A Model for when Disclosure Helps Security: What Is Different About Computer and Network Security?*, 3 J. ON TELECOMMS. & HIGH TECH. L. 163, 165 (2004) [hereinafter Swire, *A Model for When Disclosure Helps Security*] ("For proponents of [open-source] software, revealing the details of the system will actually tend to improve security, notably due to peer review. On this view, trying to hide the details of the system will tend to harm security because attackers will learn about vulnerabilities, but defenders will not know where to patch the vulnerabilities.").

[25] David Matthews, *Germany To Launch Sovereign Tech Fund To Secure Digital Infrastructure*, SCI. BUS. (May 31, 2022), https://sciencebusiness.net/news/germany-launch-sovereign-tech-fund-secure-digital-infrastructure [https://perma.cc/XXE3-U98A].

[26] Amanda Brock, *Summer of Open Source Software Security*, OPENUK (July 1, 2022), https://openuk.uk/launching-the-openuk-summer-of-open-source-software-security/ [https://perma.cc/CM6P-X94C].

[27] EUR. COMM'N, COMMUNICATION TO THE COMMISSION: OPEN SOURCE SOFTWARE STRATEGY 2020 – 2023, at 3 (Oct. 21, 2020) [hereinafter OPEN SOURCE SOFTWARE STRATEGY], https://commission.europa.eu/system/files/2020-10/en_ec_open_source_strategy_2020-2023.pdf [https://perma.cc/MLC8-7QQX].

[28] *See* KNUT BLIND, MIRKE BÖHM, PAULA GRZEGORZEWSKA, ANDREW KATZ, SACHIKO MUTO, SIVAN PÄTSCH & TORBEN SCHUBERT, EUROPEAN COMM'N, THE IMPACT OF OPEN SOURCE SOFTWARE AND HARDWARE ON TECHNOLOGICAL INDEPENDENCE, COMPETITIVENESS AND INNOVATION IN THE EU ECONOMY 15–16 (2021), https://op.europa.eu/en/publication-detail/-/publication/29effe73-2c2c-11ec-bd8e-01aa75ed71a1/language-en [https://perma.cc/B8KJ-BD44] (reporting on the economic impact of open-source technology). *See generally* OPEN SOURCE SOFTWARE STRATEGY, *supra* note 27 (describing holistic open-source strategy).

Open source's security problem is exacerbated by irresponsible users. Despite dire warnings, many organizations continue to drag their feet in implementing the *free* and *publicly available* patches that would secure their systems against threats.[29] In fact, thirty percent of organizations had not even begun to look for Log4Shell in their systems nearly two weeks after the vulnerability was identified, exposing millions of end-users to the effects of potential exploits.[30] Over four months later, sixty percent of the hundreds of millions of devices affected by the Log4Shell vulnerability were still unpatched and vulnerable[31] despite hackers continuing to exploit Log4Shell.[32] Nearly a year later, Iranian hackers exploited an unpatched version of Log4j in a federal agency's systems.[33]

Although all software has a security problem, open source's security problem is distinct due to its unique characteristics. Open source is different from closed-source software in the way it is developed, the structure of the community that supports it, and the licenses it uses for distribution. These distinctions have made open source indispensable and ubiquitous, including in our most critical infrastructure. But they also exacerbate the severity and implications of open source's security problem; open source is not governed by the market incentives that motivate companies to invest in closed-source software. Unaddressed, open source's resource deficit threatens to take the most important functions of critical systems—their public safety, economic stability, and national security—offline.

[29] Yoran, *supra* note 3; Joseph Marks, *Cyber World Is Starting 2022 in Crisis Mode with the Log4j Bug*, WASH. POST (Jan. 3, 2022, 7:30 AM), https://www.washingtonpost.com/politics/2022/01/03/cyber-world-is-starting-2022-crisis-mode-with-log4j-bug/ [https://perma.cc/YFP5-QCZY (dark archive)] [hereinafter Marks, *Cyber World*] ("Most vulnerable computer systems at prominent organizations that face the public Internet have probably been patched at this point, Williams estimated. Those that aren't patched have almost certainly been penetrated by hackers looking to steal data, steal computing power to mine cryptocurrency or for other nefarious purposes.").

[30] Yoran, *supra* note 3; Marks, *Cyber World*, *supra* note 29.

[31] YOTAM PERKAL, REZILION, LOGSHELL 4 MONTHS LATER: ARE YOU STILL VULNERABLE? 2 (2022), https://www.rezilion.com/blog/months-later-are-you-still-vulnerable-to-log4shell/ [https://perma.cc/C5UW-5GTU (staff-uploaded archive)] (click hyperlinked "this report today" and input requested information to download report); Lily Hay Newman, *The Log4j Vulnerability Will Haunt the Internet for Years*, WIRED (Dec. 13, 2021, 8:34 PM), https://www.wired.com/story/log4j-log4shell/ [https://perma.cc/N6SL-KWPS] [hereinafter Newman, *Log4j Vulnerability*] (stating that Log4J impacted hundreds of millions of devices).

[32] *See Malicious Cyber Actors Continue To Exploit Log4Shell in VMware Horizon Systems*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (June 23, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-174a [https://perma.cc/4CYW-4BN5].

[33] Graham, *supra* note 9.

Securing open source has never been more urgent.[34] However, to date, there is a dearth of literature analyzing the market failures of open source as a critical infrastructure security issue. This Article hopes to fill that gap and shed light on the value of open source, the urgency of its security problem, and the need for comprehensive, decisive government regulation. Part I begins with a description of the features that distinguish open-source from closed-source code, their benefits, and the risks they present. It continues to argue that open source is more than a novelty of the software world; it is inextricably tied to critical infrastructure and should be treated as such.

Part II explains that, to protect critical infrastructure, it is necessary to first understand the origins of the open-source security issue and the barriers to its resolution. This part characterizes open source as an impure public good that is subject to market failures endemic to public goods. It concludes that open source's market failures result in an underresourced open-source community and a lack of private sector investment in reasonable security practices—both contributing to unresolved vulnerabilities in our critical infrastructure. It identifies Irresponsible Consumers—open-source beneficiaries that fail to contribute to its production and maintenance—as central to the problem and key to the solution.

Part III uses the public goods analysis to review the effectiveness of current government interventions. Open source's market failures present a complex problem that demands a coordinated, comprehensive response. However, this part argues, open source's beneficiaries lack the incentive to take on the costs of coordination or adopt any measures to rectify the market failures, which has rendered the private sector's efforts ineffective. Government can, as it has in the past, play an integral role in the resolution of these market failures. However, this part contends its interventions to date fall short because they

[34] *Open-Source Software Usage Slowing Down for Fear of Vulnerabilities, Exposure, or Risks*, HELPNETSECURITY (Sept. 20, 2022), https://www.helpnetsecurity.com/2022/09/20/open-source-security-concerns/ [https://perma.cc/X3GG-9W2J] ("While most organizations use open source software, of the 8% of respondents whose organizations are not, 54% said the biggest reason is fear of potential vulnerabilities, exposures, or risks. This is a 13% increase from the 2021 report, reaffirming the escalated security awareness across the industry in 2022."); Joseph Marks, *Elevated Cyber Threats Are the 'New Normal,'* WASH. POST (June 7, 2022, 7:33 AM), https://www.washingtonpost.com/politics/2022/06/07/elevated-cyber-threats-are-new-normal/ [https://perma.cc/R8TX-H8L8 (dark archive)] [hereinafter Marks, *Elevated Cyber Threats*] ("More frequent cyberattacks are the 'new normal' for U.S. companies and individuals, the Biden administration's top cyber officials are warning."); *see also* Joseph Marks, *The U.S. Isn't Getting Ahead of the Cyber Threat, Experts Say*, WASH. POST (June 6, 2022, 7:31 AM), https://www.washingtonpost.com/politics/2022/06/06/us-isnt-getting-ahead-cyber-threat-experts-say/ [https://perma.cc/4N3V-Q6BX (dark archive)] [hereinafter Marks, *The U.S. Isn't Getting Ahead*] ("About 43 percent of respondents to [the *Washington Post*'s] Network experts poll said the United States is more vulnerable to cyberattacks now.").

have been piecemeal and incomplete.[35] This part concludes that without the introduction of strong incentives or legal mandates, any intervention will have limited success. There is no silver-bullet solution to this complex problem; but this Article begins a conversation that is long overdue on an issue of national importance.

I. WHAT IS OPEN SOURCE AND WHY DOES IT MATTER?

All software has a security problem; vulnerabilities are inevitable. However, open source's security problem is unique. Its differences from closed-source software give rise to its distinctive benefits and potential, which have in turn led to its incorporation in most of society's technology, including our most critical infrastructure. But its differences also exacerbate the scope and severity of open source's vulnerabilities. This part proceeds in two sections. Section A analyzes the benefits and security challenges associated with its defining characteristics. Section B makes the case that, given open source's role in modern society, it constitutes critical infrastructure.

A. *Open Source's Differences from Closed-Source Code*

Understanding how open source differs from closed-source software is critical to understanding its unique challenges for security. This subsection engages in those primary differences. The first is the ways users interact with the code—that is how the code is used and written. Open-source code is free and is prime for innovative collaboration. Closed-source code—not so much. The second difference is the community that writes the code. A variety of entities and people write open-source code, and these support structures and developers are critical not just to its success, but its security as well. Finally, the subsection delves into the licenses governing the code. As compared to traditional proprietary, closed-source code, open-source code confers unenforceable property rights: the right of exclusion is tenuous at best.

1. Writing and Using Open-Source Code

As a preliminary matter, it is important to clarify that open-source code is exactly that: code. Software (i.e., code) is a set of commands that are ultimately translated into 1s and 0s and tell a computer what to do.[36] In this regard, open-source code is no different from closed-source code. One of its defining features is that anyone can see it, use it, and contribute to it. Closed-source code, on the

[35] *See infra* Section III.B.2.

[36] Klaus M. Schmidt & Monika Schnitzer, *Public Subsidies for Open Source—Some Economic Policy Issues of the Software Market*, 16 HARV. J.L. & TECH. 473, 475 (2003).

other hand, is privately controlled.[37] Open source's distinguishing qualities offer benefits over closed-source code, but also introduce challenges and complications.

a. Open Sourcing Code

Code becomes open source when its developer introduces it to the "digital commons." Open sourcing a project entails more than providing public access to the source code; it means permitting the free and technology-neutral[38] redistribution of the code, the creation and distribution of derivative code, and the indiscriminate use of the code by all persons or for any purpose.[39] These conditions are enshrined in valid open-source licenses.[40]

To open source a project, a developer must first provide public access to the source code, usually by moving it, or "pushing it," from a developer's computer to a centralized hosting platform and making that project public.[41] There are many hosting services, but the most popular is GitHub,[42] which simplifies the use of Git, an open-source version control technology.[43] Once the source code is made public and the developer attaches a valid open-source license to the project, it enters the digital commons and the developer surrenders control. Using Git, anyone can copy, or "pull," an open project onto their local computer, where they are free to review, use, change, or contribute to it.[44] Licenses may dictate the legally permissible uses of an open-source project;[45] but technologically speaking, once a project is open, its code is out of the developer's control.

[37] *What Is Open Source?*, OPENSOURCE.COM, https://opensource.com/resources/what-open-source [https://perma.cc/9549-SHCR].

[38] "No provision of the license may be predicated on any individual technology or style of interface." *The Open Source Definition*, OPEN SOURCE INITIATIVE, https://opensource.org/osd [https://perma.cc/4Z9B-4VSX].

[39] *Id.*

[40] *Starting an Open Source Project*, OPEN SOURCE GUIDES, https://opensource.guide/starting-a-project/ [https://perma.cc/A6R2-JSZD].

[41] Projects on the internet can be private.

[42] Emma Witman, *What Is GitHub? How To Start Using the Code Hosting Platform That Allows You To Easily Manage and Collaborate on Programming Projects*, INSIDER (June 29, 2021, 12:45 PM), https://www.businessinsider.com/what-is-github [https://perma.cc/SXP8-G474].

[43] GIT, https://git-scm.com/ [https://perma.cc/W33T-BZJ5].

[44] *See generally Open Project*, GITHUB, https://github.com/opf/openproject [https://perma.cc/86SC-RQEH] ("OpenProject is the leading open source project management software."); *Manage Projects Hosted on GitHub*, JETBRAINS (Dec. 21, 2022), https://www.jetbrains.com/help/phpstorm/manage-projects-hosted-on-github.html [https://perma.cc/74FE-HG94] (describing the process of GitHub Open Project integration).

[45] *See infra* Section II.A.3.

b. The Value of Using Open Source

Open source's most obvious value is that it makes innovative, useful software available to anyone for free. This software can be as simple and discrete as a project that automates right-justifying text.[46] Or it can be as complex and comprehensive as Stable Diffusion, the open-source artificial intelligence project that can produce a plethora of digital art with nothing more than a simple, one-line text prompt.[47] Developers deliver substantial value to society by donating original software to the digital commons.

These projects can be used by hobbyists, but for the most part, they are incorporated into commercial software—closed-source code for sale or otherwise supporting a commercial purpose. Almost every highly profitable company uses some amount of open-source code in commercial products or services.[48] It is easy to see why. For example, say one is building a Microsoft Word competitor and needs to write the code that right-justifies text when a user pushes the right-justify button. There are two options. The user could pull an open-source project and, essentially, copy and paste that code into their commercial product. Or they can reinvent the wheel and build their own closed-source code to do the same thing.

Using freely available software that accomplishes a needed function saves developers time. Companies profit when their developers are freed up to focus on high-value work rather than garden-variety software development work.[49] These benefits are amplified for small- and medium-sized organizations.[50] Beyond avoiding tedium, using open source also gives developers access to advanced technology they may not have been able to build themselves, such as AI. Developers (and their employers) reap the benefit of software ingenuity, which can in turn foster more innovation.[51] A company not only gains access to

[46] Sean Gallagher, *Rage-Quit: Coder Unpublished 17 Lines of Javascript and "Broke the Internet*,*"* ARS TECHNICA (Mar. 24, 2016, 10:10 PM), https://arstechnica.com/information-technology/2016/03/rage-quit-coder-unpublished-17-lines-of-javascript-and-broke-the-internet/ [https://perma.cc/FW79-DED3].

[47] *Stable Diffusion 2 Demo*, HUGGING FACE, https://huggingface.co/spaces/stabilityai/stable-diffusion [https://perma.cc/2K6S-64RR].

[48] *See* 2022 SYNOPSYS REPORT, *supra* note 16, at 5–8.

[49] Ben Balter, *6 Motivations for Consuming or Publishing Open Source Software*, OPENSOURCE.COM (Dec. 9, 2015), https://opensource.com/life/15/12/why-open-source [https://perma.cc/84UK-459V].

[50] *See* BLIND ET AL., *supra* note 28, at 199 ("Furthermore, micro and small and medium-sized organisations rank the benefits higher than large organisations. In particular, small and medium-sized organisations rate the revenue opportunities and the access to new markets above medium and therefore higher both than micro and large organisation.").

[51] *Id.* at 15–16 (calculating the return on one billion euros of investment in open source as a sixty-five billion to ninety-five billion euro return in GDP growth and, after taking into account hardware and other capital costs, the cost-benefit ratio for open source is slightly above 1:4);

the functionality of this cutting-edge code, but its developers also learn from it. They are able to view how the code was built, thus building new skills and thereby increasing their worth. These advantages compound and have network effects.[52]

A related feature of open-source projects is that they are modular (built to interoperate with other software) because open-source developers want to maximize the usability of the code for all known and unknown use cases.[53] Think of open-source projects as Lego blocks; by fitting pieces together, a company can build something that fits their needs and change a piece out when it no longer serves them. In this way, open source allows companies to be agile and responsive to technological advancements and market trends.[54] By contrast, closed-source, proprietary code tends not to be as interoperable; companies can profit more when they can sell a suite of solutions and build a customer's dependency on them.[55] The software industry is unique in that it has the right to prohibit reverse engineering its products—I can take apart a computer to

JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 64 (2008) ("Our information technology ecosystem functions best with generative technology at its core. A mainstream dominated by non-generative systems will harm innovation as well as some important individual freedoms and opportunities for self-expression. However, generative and non-generative models are not mutually exclusive. They can compete and intertwine within a single system. For example, a free operating system such as GNU/Linux can be locked within an information appliance like the TiVo, and classical, profit-maximizing firms like Red Hat and IBM can find it worthwhile to contribute to generative technologies like GNU/Linux. Neither model is necessarily superior to the other for all purposes. Moreover, even if they occupy a more minor role in the mainstream, non-generative technologies still have valuable roles to serve. But they develop best when they can draw on the advances of generative systems.").

[52] JONATHAN E. NUECHTERLEIN & PHILIP J. WEISERS, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 333 (2005); Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSPS. 2, 93, 96–100 (1994); *see also* Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 3, 424, 436 (1985).

[53] Fernando Almeida, José Oliveira & José Cruz, *Open Standards and Open Source: Enabling Interoperability*, 2 INTL. J. SOFTWARE ENG'G & APPLICATIONS 1, 8 (2011) ("Market experience with OSS to date does not demonstrate significant, irresolvable interoperability problems with the most widely used popular OSS applications. One rational explanation for this is that open-source developers are gathering together to solve generic problems they share. Open source is not only a piece of software but it is also a process to build and license code in order to solve common shared problems such as infrastructure problems.").

[54] *Manage Vulnerabilities in ICS Open Source Software*, GLOB. CYBERSECURITY ALL., https://gca.isa.org/blog/manage-vulnerabilities-in-ics-open-source-software [https://perma.cc/JD6X-T8LR] ("OSS provides great interoperability, portability, and interchangeability to ICS, as numerous devices may all come from different vendors in the supply chain with heterogeneous software packages. The 'open' nature of OSS allows ICS providers and industrial device suppliers to integrate systems with ease and flexibility while effectively enhancing the efficiency of software development without building things up from scratch.").

[55] Kevin Xiaoguo Zhu & Zach Zhizhong Zhou, *Lock-In Strategy in Software Competition: Open-Source Software vs. Proprietary Software*, 23 INFO. SYS. RSCH. 536, 536 (2012).

inspect its different parts, but I am not allowed to take apart and reconfigure software.[56] This leads to vendor lock-in—by licensing closed-source, proprietary software, a consumer cannot benefit from the new features developed by a competitor or open-source developer, since replacing or rewriting one component can break other dependent components—like Jenga.[57]

Open source also saves developers the time it takes to maintain a project. All projects, whether open or closed, require maintenance. Project or software maintainers do this work, monitoring the project for contributions, resolving conflicts, responding to bug reports, scanning for issues, and developing patches.[58] Given software's dynamic nature, this task never ends. With closed-source code, if the developer does not maintain the code, no one else can. With open-source code, a developer using an open-source project can benefit from updates to the code made by the maintainer.

c. *The Ability To Crowdsource Project Support*

Open source is built to evolve, and its projects benefit from the fact that anyone and everyone can contribute to them. Generally, all software projects have multiple developers working on them.[59] With closed-source projects, contributions are limited to a defined, private group of developers. With open source, anyone, not just the developers who originally open-sourced the software, can contribute to the code.[60]

Open-source developers can generate value by paying it forward (building off an existing open-source project) or paying it back (contributing to the maintenance of an existing open-source project). The Git "fork" functionality allows developers to make a copy of the code, which they can choose to open

[56] This is primarily accomplished contractually, through restrictions included in the End User License Agreements ("EULA") a company uses to distribute its software. Davidson & Assocs. v. Jung, 422 F.3d 630, 633–35 (8th Cir. 2005). *But see* Sega Enters. v. Accolade, Inc., 977 F.2d 1510, 1531 (9th Cir. 1992); Sony Comput. Ent., Inc. v. Connectix Corp., 203 F.3d 596, 609 (9th Cir. 2000).

[57] *See* BLIND ET AL., *supra* note 28, at 296; *see also* Schmidt & Schnitzer, *supra* note 36, at 473, 490.

[58] *See What's an Open Source Software Maintainer?*, FOSSLIFE (June 23, 2021), https://www.fosslife.org/whats-open-source-software-maintainer [https://perma.cc/HS27-TSQK] (describing how "maintainers" "build[] new features," "writ[e] code," "bug reports," and "improv[e] existing code," among other tasks).

[59] *See* Schmidt & Schnitzer, *supra* note 36, at 482.

[60] *Id.* at 484.

source.[61] There, they can make customizations without affecting the original project, and allow others to use or modify this new version.[62]

Instead of creating a new project, an open-source developer can contribute back to a project they find useful without having any relation to the original developers. For example, a security researcher can inspect a project on their own fork. They can do more than just report a vulnerability they found; forking allows them to fix the issue themselves—rewriting the code on their own fork and then making a "pull request" to submit the solution to the project owner.[63] At this juncture, the project owner can review the changes and, if comfortable, they can "merge" the fork with the original version, publishing the changes to the master copy.[64]

Git allows thousands of developers to contribute in tandem to the same project.[65] This means that multiple people can be looking for vulnerabilities and "patching" or fixing them. A famous adage in the open-source community is Linus's Law, which states that "many eyes make all bugs shallow."[66] In this way, open source can improve project security—instead of relying on a small team of developers to review closed-source code for bugs and vulnerabilities, an open-source project benefits from the eyes of an entire community.[67]

[61] *See* Cameron McKenzie, *Git Fork vs. Clone: What's the Difference?*, TECHTARGET (July 28, 2021), https://www.theserverside.com/answer/Git-fork-vs-clone-Whats-the-difference [https://perma.cc/Q3WM-CPBL] ("A fork creates a completely independent copy of Git repository.").

[62] *See id.* (describing how after a fork "changes and updates to the forked repository will be isolated to the fork and will not be reflected in the original repo").

[63] Jake Jarvis, *How To: Fork a GitHub Repository & Submit a Pull Request*, JARV.IS (Apr. 9, 2019), https://jarv.is/notes/how-to-pull-request-fork-github/ [https://perma.cc/3UR2-Y9GP].

[64] *See* P0dalirius, *Fix LDAP Attributes with a List of Strings Not Populating, Closes #2*, GITHUB (May 2, 2022), https://github.com/p0dalirius/ldap2json/pull/3 [https://perma.cc/58RY-4D3F] (providing an example of a fork, describing the issue it is resolving, and the fork being merged into the master copy of a very popular open-source project after the maintainer reviewed and approved it).

[65] *See A Guide to the Kernel Development Process*, LINUX KERNEL, https://www.kernel.org/doc/html/latest/process/1.Intro.html [https://perma.cc/YJ5K-W8PQ].

[66] Jeff Jones, *Linus's Law aka "Many Eyes Make All Bugs Shallow*,*"* MICROSOFT SEC. (June 7, 2006), https://www.microsoft.com/security/blog/2006/06/07/linuss-law-aka-many-eyes-make-all-bugs-shallow/ [https://perma.cc/DL3V-T8F3].

[67] *Id.* Sonali Shah & Frank Nagle, *Why Do User Communities Matter for Strategy?* 11 (Harv. Bus. Sch. Strategy Unit Working Paper No. 19-126, 2019) [hereinafter Shah & Nagle, *Why Do User Communities Matter for Strategy?*], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3407610 [https://perma.cc/WWZ8-FLTE (staff-uploaded archive)] (click "Download This Paper") ("Openness and fluidity benefit the community, as new or infrequent participants bring in new problems to be solved as well as new knowledge and insights that might be helpful in generating solutions."); *see also* Swire, *A Model for When Disclosure Helps Security*, *supra* note 24, at 165 ("For proponents of Open Source software, revealing the details of the system will actually tend to improve security, notably due to peer review. On this view, trying to hide the details of the system will tend to harm security because attackers will learn about vulnerabilities, but defenders will not know where to patch the vulnerabilities.").

The open-source model compellingly challenges the long-held maxim that security is best achieved through obscurity.[68] Excepting a limited set of circumstances, the open-source community lives by the principle that transparency and open disclosure give hackers little advantage and greatly benefit developers defending projects.[69] Openness is both more likely to prevent the first attack, because more developers looking for bugs makes it less likely a bad actor finds one first, and it is more likely to mitigate the fall-out of an attack, because once the vulnerability is publicly disclosed, all other users of the code are given equal opportunity to protect themselves.[70]

In addition to collaboration and security benefits, the open-source model can also enable the smooth transition from one project maintainer to another. Sometimes the developer who first posted a project abandons post; they wanted to share their code, not take care of it forever. These projects still have users who rely on them, but they can remain dormant for years, unresolved bug reports and vulnerability disclosures piling up.[71] These are called orphan projects,[72] and they are especially susceptible to attack.[73] Open source's unique capabilities provides the solution: in theory, another developer can fork the project, take over as maintainer, and encourage the original project's users to pull from the new copy instead. The open-source community has even set up

[68] *See also* Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333, 1337–42 (2006) [hereinafter Swire, *A Theory of Disclosure for Security and Competitive Reasons*] ("In short, obscurity may work against the first attackers, but will not work once the attackers learn to watch for the hidden pit."). *See generally* Shah & Nagle, *Why Do User Communities Matter for Strategy?*, *supra* note 67 (describing the impact of community involvement in developing open-source security measures).

[69] Swire, *A Theory of Disclosure for Security and Competitive Reasons*, *supra* note 68, at 1347–51 (describing the use of intrusion detection software and "honeypots" that, unbeknownst to a bad actor, are surveilling for suspicious activity and deceiving hackers into attacking decoys rather than the real projects).

[70] However, as discussed at length below, this assumption does not always hold water because irresponsible vendors fail to take advantage of their head start and because deeply embedded dependencies can be hard to find and therefore hard to fix.

[71] DAVID REID, MAHMOUD JAHANSHA & AUDRIS MOCKUS, THE EXTENT OF ORPHAN VULNERABILITIES FROM CODE REUSE IN OPEN SOURCE SOFTWARE 9 (2022), https://conf.researchr.org/details/icse-2022/icse-2022-papers/186/The-Extent-of-Orphan-Vulnerabilities-from-Code-Reuse-in-Open-Source-Software [https://perma.cc/KU8N-JKBB] (concluding that orphan vulnerabilities persist in popular projects that have lied dormant for years).

[72] *See* *GitAbandonWare*, ABANDONWARE, https://abandonware.github.io/ [https://perma.cc/6PGB-RK7N].

[73] Ax Sharma, *Popular Python and PHP Libraries Hijacked To Steal AWS Keys*, BLEEPINGCOMPUTER (May 24, 2022, 7:42 AM), https://www.bleepingcomputer.com/news/security/popular-python-and-php-libraries-hijacked-to-steal-aws-keys/ [https://perma.cc/EYX9-L2Z7] (describing the attack of library that gets downloaded over 20,000 times a week but has not been touched since 2014 as an example of "repojacking," when a maintainer changes their username, allowing any third party to claim their old name linked to the library and take over the account for malicious purposes).

organizations that attempt to collect orphan projects and find support for them.[74]

d. *The (Alleged) Pitfalls of Openness*

Although open source is arguably more secure than closed-source code,[75] approximately eighty-one percent of software programs containing open source still have at least one vulnerability.[76] Because everyone can contribute to the code, anyone can contribute vulnerable code. Because the code is universally accessible, users and maintainers may never know each other. Because of this opacity problem, users may not even know what they are using or that they are at risk. And because open source is everywhere, any threat is amplified.

There is a low barrier to entry for open-source contributions, which means projects can benefit from a wider pool of talent; but it also means there are no assurances as to the abilities or intentions of the contributor and the quality of the project. An amateur developer can unwittingly contribute useful, but vulnerable, code. A malicious developer might do the same, but intentionally.[77] Even the most sophisticated developers can inadvertently contribute insecure code; writing useful code and writing secure code are distinct skills. Thorough reviews of code contributions by maintainers can mitigate these risks, but just as anyone can be a developer, anyone can be a maintainer—an amateur maintainer would miss the vulnerability and a bad actor would welcome it.

Open source necessitates public disclosures of vulnerabilities; when you do not know who to notify about a bug, you have to notify everyone. While the merits of a "security by obscurity" model are disputed, a highly controlled environment would theoretically allow organizations to contain vulnerability information to a small group of known, trusted customers, giving them time to

[74] *Id.*

[75] *See* HENDRICK & MCKEAY, *supra* note 21, at 19 (finding that over half of all bugs found were in software developed in-house as opposed to third-party software, such as an open-source component); Michael M. Lokshin, Sardar Azari & David Newsom, *Quality of Open Source Software: How Many Eyes Are Enough?*, WORLD BANK BLOGS (Jan. 24, 2019), https://blogs.worldbank.org/opendata/quality-open-source-software-how-many-eyes-are-enough [https://perma.cc/RB5H-954H] (finding that the number of bugs per 1,000 lines of code was smaller for open-source than closed-source software).

[76] 2022 SYNOPSYS REPORT, *supra* note 16, at 10.

[77] Jule Pattison-Gordon, *U.S. House Lawmakers Search for Open Source Security Fixes*, GOV'T TECH. (May 13, 2022), https://www.govtech.com/security/u-s-house-lawmakers-search-for-open-source-security-fixes [https://perma.cc/GGP8-XA3B] ("Because anyone can submit open source code, Lohn said there's a risk that malicious contributors will try to abuse the process, such as by poisoning the data on which AI models train or by inserting hard-to-detect backdoors into pieces of open source software that would allow hackers to later compromise final projects.").

fix the issue before anyone comes to harm.[78] With commercial code, sales produce a paper trail of transactions—a company knows its customers, giving it the ability to carefully control the vulnerability disclosure process.[79] No such *closed* circle of trust exists for open source. The ease with which projects can be pulled or forked using Git has allowed open source to flourish, but it also obfuscates the location and uses of any given project. Neither maintainers nor users of a project know where the code is and what it is being used for, which precludes privately notifying other affected parties of an issue, distributing a fix, collaborating on development, or preventing use of an insecure project version.[80] Apple has the benefit of knowing its customers; when an iOS update is out, it notifies every user. There is no analogous push notification for open source.

Between open source's opacity problem and the complexity of the software supply chain, downstream users are often unaware of the software components they are using and who wrote them.[81] Because open source is modular, it is like a Russian doll: one project can be dependent on another project, which is dependent on a third project. Software dependencies are nested and harder to find. Developers are unlikely to review every line of dependency code when they pull a project they need or acquire software from a third-party. But the unreviewed dependencies can contain several other undocumented libraries with vulnerabilities. Even if a diligent developer attempted to identify all the open-source components using advanced dependency-scanning software, a

[78] *See* Swire, *A Theory of Disclosure for Security and Competitive Reasons*, *supra* note 68, at 1338 ("In contrast, the military assumptions highlight the ways that disclosure will assist the attackers. For a military base, for instance, the precise location of machine guns and other defenses is closely guarded. A major goal is to hide the defenses until it is too late for attackers so that they fall into traps. In terms of disclosure helping defenders, the military traditionally uses its chain of command to tell fellow defenders what they need to know. There is no general broadcast of security flaws because such a broadcast would help the attackers but provide little or no information to fellow defenders.").

[79] The government uses this ability to stockpile vulnerabilities. Private companies use this to keep vulnerabilities they discover confidential, as there is no vulnerability reporting requirement. The number of private sector incidents and vulnerabilities is impossible to know, as much of the relevant information is kept held close.

[80] *See* Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 937 (2005) (discussing how ignorance is built into a commons ecosystem).

[81] "[T]he complexity of the ICT supply chain has led many Original Equipment Manufacturers (OEMs) to outsource firmware development to third party suppliers, which introduces risks related to the lack of transparency into suppliers' programming and cybersecurity standards." U.S. DEP'T OF COM. & U.S. DEP'T OF HOMELAND SEC., ASSESSMENT OF THE CRITICAL SUPPLY CHAINS SUPPORTING THE U.S. INFORMATION AND COMMUNICATIONS TECHNOLOGY INDUSTRY 3 (2022), https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf [https://perma.cc/JH6D-SPLF]. "In many instances, the author of a given open-source software component is unknown." *Id.* at 34.

buried dependency may not be found.[82] Log4j, for instance, was a library embedded so many layers deep that even sophisticated companies, such as Google, did not find it in routine vulnerability scans.[83] When the developer uses this open-source code in a final product, the risk of a vulnerable dependency is shifted to the consumer.

What makes open source valuable also makes it a unique risk.[84] Software vulnerabilities are inevitable. But, with closed-source, proprietary software, a vulnerability would only impact that company and its customers. While these threats are still severe,[85] they are generally outmatched in scope by a vulnerability found in open-source software. When the same piece of code is used by hundreds of thousands of networks internationally, then one vulnerability in one project can take countless critical systems offline.[86]

Hackers are specifically targeting open-source projects because of this domino effect. One report noted a 650% increase year-over-year in cyberattacks aimed at vendors using open-source software in 2021.[87] Researchers attributed the spike to hackers using vulnerabilities in upstream vendors to exploit all their downstream customers.[88] Similarly, "account takeover" attacks, where a bad

[82] Joe Uchill, *Warning: Log4j Still Lurks Where Dependency Analysis Can't Find It*, SC MEDIA (Jan. 5, 2022), https://www.scmagazine.com/analysis/vulnerability-management/warning-log4j-still-lurks-where-dependency-analysis-cant-find-it [https://perma.cc/J9H4-Q2JP].

[83] James Wetter & Nicky Ringland, *Understanding the Impact of Apache Log4j Vulnerability*, GOOGLE SEC. BLOG (Dec. 17, 2021), https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html [https://perma.cc/B4CS-UX8N].

[84] Martin Hell & Martin Höst, *Communicating Cybersecurity Vulnerability Information: A Producer-Acquirer Case Study*, *in* PRODUCT-FOCUSED SOFTWARE PROCESS IMPROVEMENT 215, 216 (Markku Oivo & Seija Komi-Sirviö eds., 2021) ("The combined increase in the use of OSS and the increase in newly found vulnerabilities puts the industry at higher risk than ever.").

[85] *See, e.g.*, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, U.S. GOV'T ACCOUNTABILITY OFF. (Jan. 13, 2022), https://www.gao.gov/products/gao-22-104746 [https://perma.cc/B2QR-PY34] (describing recent high-profile cybersecurity incidents affecting the government).

[86] Tatum Hunter & Gerrit De Vynck, *The 'Most Serious' Security Breach Ever Is Unfolding Right Now. Here's What You Need To Know*, WASH. POST (Dec. 20, 2021, 5:28 PM), https://www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java/ [https://perma.cc/S4A6-TK5Z (dark archive)] ("The fact that log4j is such a ubiquitous piece of software is what makes this such a big deal. Imagine if a common type of lock used by millions of people to keep their doors shut was suddenly discovered to be ineffective. Switching a single lock for a new one is easy, but finding all the millions of buildings that have that defective lock would take time and an immense amount of work."); REID ET AL., *supra* note 71, at 10 (stating the results of a study which found that the ability to copy an open-source project for individual use led to the spread of vulnerabilities, compromising every project that reused the code).

[87] 2021 SONATYPE REPORT, *supra* note 20, at 4.

[88] *Id.*

actor uses a maintainer's account to inject a project with malicious code, have become the second largest threat to open source.[89]

While one iOS vulnerability might have comparable scope, that risk is multiplied by the high number of open-source projects with iOS-level popularity. The open-source ecosystem has an unparalleled attack surface.[90]

2. The Community Building Open Source

As should be clear by now, open source is more than code—it is also the community that builds the code. The open-source community includes the individuals, nonprofits, and companies actively contributing to open source's continued production. To understand the community's role in securing open source, it is critical to first understand its motivations, structure, capabilities, and limitations.

a. Open Source's Developers

In the early age of open source, the community was composed almost entirely of volunteers.[91] Today, it includes volunteer hobbyists, nonprofit-funded developers, dedicated corporate professionals, and government employees.[92] Throughout, the dominant motivator for open-source

[89] RUIAN DUAN, OMAR ALRAWJ, RANJITA PAI KASTURI, RYAN ELDER, BRENDAN SALTAFORMAGGIO & WENKE LEE, TOWARDS MEASURING SUPPLY CHAIN ATTACKS ON PACKAGE MANAGERS FOR INTERPRETED LANGUAGES 5 (2021), https://arxiv.org/abs/2002.01139 [https://perma.cc/U34Q-35PF].

[90] MICHAEL SCOVETTA, THREATS, RISKS, AND MITIGATIONS IN THE OPEN SOURCE ECOSYSTEM 6 (2020), https://github.com/ossf/wg-identifying-security-threats/blob/main/publications/threats-risks-mitigations/v1.1/Threats%2C%20Risks%2C%20and%20 Mitigations%20in%20the%20Open%20Source%20Ecosystem%20-%20v1.1.pdf [https://perma.cc/T75L-2V8Y] ("As a system's attack surface grows or becomes less well-defined, it becomes more susceptible to attack. . . . Systems that have many dependencies could be attacked using a defect in any of them.").

[91] Jesus M. Gonzalez-Barahona, *A Brief History of Free, Open Source Software and Its Communities*, 54 COMPUT. 75, 76 (2021) ("[In the 1980's, the first major open-source project] work was structured in small teams of volunteers who produced different pieces of software . . . .").

[92] *See* Mario Schaarschmidt & Harald Von Kortzfleisch, *Firms' Resource Deployment and Project Leadership in Open Source Software Development*, INT'L J. INNOVATION & TECH. MGMT., Oct. 23, 2014, at 1, 3–4; Linus Dahlander & Mats G. Magnusson, *Relationships Between Open Source Companies and Communities: Observations from Nordic Firms*, 34 RSCH. POL'Y 481, 481–92 (2005); Pankaj Setia, Balaji Rajagopalan, Vallabh Sambamurthy & Roger Calantone, *How Peripheral Developers Contribute to Open-Source Software Development*, 23 INFO. SYS. RSCH. 144, 144–45 (2012); Sebastian Spaeth, Georg von Krogh & Fang He, *Perceived Firm Attributes and Intrinsic Motivation in Sponsored Open Source Software Projects*, 26 INFO. SYS. RSCH. 224, 224 (2015) ("In September 2013, IBM announced plans to invest US $1 billion in new Linux and open source technologies for its Power Systems servers. Besides the vast investment of IBM, the development of the latest Linux kernel (version 3.14) includes contributions by more than 200 other firms, according to LWN.net. Firms pledge substantial financial, human, and technological resources to the project with objectives such as increasing sales, improving reputation, cutting product development cost, shortening time to market of new products, and detecting new technologies and user needs.").

contributions has been the sense of joy, altruism, and accomplishment tied to the activity.[93] Obvious extrinsic factors drive open-source development as well: developers build software they need;[94] developers can learn from a worldwide community of experts;[95] a developer can improve their reputation[96] and employability.[97] In a recent report, eighty-nine percent of respondents reported feeling their contributions had a positive impact on the world.[98] Public goods theory assumes that "the only motive that an individual has to provide units of such a [public] good is his or her own private motive of present or future consumption. Enjoyment of those units by others is an incidental by-product."[99] Not so for open source. They build projects for the specific purpose of placing them in the digital commons.[100]

Closed-source code, on the other hand, is usually built by paid developers who cater to their employer's interests. Paid developers cannot work on whatever they find interesting—they must work on whatever best serves the company. From the employer's perspective, the closed-source code their organization develops costs them the amount of their developers' salaries and

[93] *See generally* Karim R. Lakhani & Robert G. Wolf, *Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects*, *in* PERSPECTIVES ON FREE AND OPEN SOURCE SOFTWARE 3 (Joseph Feller, Brian Fitzgerald, Scott A. Hissam & Karim R. Lakhani eds., 2005) (discussing motivations and drivers behind creating free or open-source software).

[94] Chorng-Guang Wu, James H. Gerlach & Clifford E. Young, *An Empirical Analysis of Open Source Software Developers' Motivations and Continuance Intentions*, 44 INFO. & MGMT. 253, 253–62 (2007).

[95] *See id.* at 259.

[96] Yuanfeng Cai & Dan Zhu, *Reputation in an Open Source Software Community: Antecedents and Impacts*, 91 DECISION SUPPORT SYS. 103, 103 (2016).

[97] *See generally* THE LINUX FOUND., THE 2021 OPEN SOURCE JOBS REPORT (2021), https://www.linuxfoundation.org/research/the-2021-open-source-jobs-report [https://perma.cc/5J4Y-JLLP] (describing the motivations for participating in user communities); *see also* Shah & Nagle, *Why Do User Communities Matter for Strategy?*, *supra* note 67, at 12 ("Career benefits can also serve as an extrinsic motivator: by participating in a user community, an individual can signal the possession of existing skills to employers, as well as learn (and signal) new skills.").

[98] HILARY CARTER & JESSICA GROOPMAN, THE LINUX FOUND., DIVERSITY, EQUITY, AND INCLUSION IN OPEN SOURCE 6 (2021), https://www.linuxfoundation.org/wp-content/uploads/LFResearch_DEISurvey_Report_121321_6.pdf [https://perma.cc/8JHU-PW2M].

[99] RICHARD CORNES & TODD SANDLER, THE THEORY OF EXTERNALITIES, PUBLIC GOODS, AND CLUB GOODS 39 (1996).

[100] Shah & Nagle, *Why Do User Communities Matter for Strategy?*, *supra* note 67, at 1, 21 (explaining that "[u]ser communities provide participants with the social context and resources to create useful and publicly available designs for physical products and copies of digital products that have inspired, extended, and even displaced commercially produced products" and that "[u]ser communities have been helpful in bringing such flaws to light and showing that a number of users are experiencing the same issue, which can occur, when, for example, an individual begins by noting a problem they have had—and then others echo the same issue").

constitutes valuable, protected intellectual property.[101] To recoup the cost, and hopefully earn a profit, companies are incentivized to sell or license the software built rather than give it away for free.

While volunteers remain a dominant force in the open-source community, over time, different motivations have brought paid professionals from the public and private sector into the fold—creating a class of Contributing Consumers. Companies consuming open source can also benefit from contributing to it by using the insight they gain from the projects to build complementary products or to influence project development in a way that supports their products.[102] For example, IBM gained strategic advantage over competitors by offering specialized hardware and software products that relied on the Linux kernel.[103]

These Contributing Consumers dedicate developers to support projects they see value in, contribute funds to maintain a project they rely on, or open source their own project to crowdsource community contribution to its maintenance.[104] Unlike their peers, these entities are actively repaying the open-source ecosystem they benefit from. Companies like IBM, Microsoft, Google, Intel, Amazon, and Meta rank among the top contributors to open source in the

[101] *See* Sonali K. Shah, *Motivation, Governance, and the Viability of Hybrid Forms in Open Source Software Development*, 52 MGMT. SCI. 1000, 1001 (2006) ("[T]he research and development efforts of most firms and independent inventors are based on a proprietary benefit model. In this model, exclusive property rights are the basis for capturing value from innovative investments. Firms and independent inventors strive to innovate in hopes of realizing profits from products protected by patents, copyrights, and/or trade secrets.").

[102] Markus Reisinger, Ludwig Ressner, Richard Schmidtke & Tim Paul Thomes, *Crowding-In of Complementary Contributions to Public Goods: Firm Investment into Open Source Software*, 106 J. ECON. BEHAV. & ORG. 78, 78–79 (2014); Frank Nagle, *Learning by Contributing: Gaining Competitive Advantage Through Contribution to Crowdsourced Public Goods*, 29 ORG. SCI. 569, 584 (2018) [hereinafter Nagle, *Learning by Contributing*] ("For managers, the results suggest that contributing to the creation of crowdsourced public goods can help increase the ability of the firm to capture value from the use of the goods.").

[103] Joel West, *How Open Is Open Enough? Melding Proprietary and Open Source Platform Strategies*, 32 RSCH. POL'Y 1259, 1259 (2003); Spaeth et al., *supra* note 92, at 224 ("In September 2013, IBM announced plans to invest US $1 billion in new Linux and open source technologies for its Power Systems servers. Besides the vast investment of IBM, the development of the latest Linux kernel (version 3.14) includes contributions by more than 200 other firms, according to LWN.net. Firms pledge substantial financial, human, and technological resources to the project with objectives such as increasing sales, improving reputation, cutting product development cost, shortening time to market of new products, and detecting new technologies and user needs."); *see* Nagle, *Learning by Contributing*, *supra* note 102, at 583–84 ("For managers, the results suggest that contributing to the creation of crowdsourced public goods can help increase the ability of the firm to capture value from the use of the goods.").

[104] DIRK HOMSCHEID, FIRM-SPONSORED DEVELOPERS IN OPEN SOURCE SOFTWARE PROJECTS 73–75 (2020).

private sector, donating employee time and money.[105] Academic institutions like the University of Michigan, nonprofits like Mozilla, and government entities are also major contributors.[106]

The open-source community's diverse participants, diffuse nature, and enormous size make organization a challenge. The community is a collective of disparate developers, of all ages and backgrounds, from all over the world,[107] most of whom have no relation to each other. There are now over seventy-three million developers on GitHub alone—sixteen million of whom joined within the past year.[108] Collectively, sixty-one million new projects were created last year.[109] This means that much of our technology relies on the coordination efforts of millions of strangers with different motivations. For many, the only interactions they have with each other occur through hosting platforms such as GitHub and electronic mailing lists.[110]

Wrangling the disparate developers who contribute to a project is not just a logistical challenge, but an incentives challenge as well. For the volunteers, it can be hard to influence their behavior given they are not being compensated for their work.[111] For paid contributors, especially corporate contributors, it can be hard for the developer to balance employer pressure to cater to company needs and the community's pressure to do what is best for the project. When paid contributors are the *only* developers on a project, then the tail begins to

[105] *Top Companies Contributing to Open Source – 2011/2021*, STAT. & DATA, https://statisticsanddata.org/data/top-companies-contributing-to-open-source-2011-2020/ [https://perma.cc/L2H9-FF5Q].

[106] *Id.*; STEPHEN D. SMALLEY, NAT'L SEC. AGENCY, INTEGRATING FLEXIBLE SUPPORT SECURITY POLICIES INTO THE LINUX OPERATING SYSTEM, https://www.nsa.gov/portals/75/documents/what-we-do/research/selinux/documentation/presentations/2005-flexible-support-for-security-policies-into-linux-os-presentation.pdf [https://perma.cc/U4MQ-9A22].

[107] *See generally* CARTER & GROOPMAN, *supra* note 98 (describing the diversity of the open-source community); FRANK NAGLE, DAVID A. WHEELER, HILA LIFSHITZ-ASSAF, HAYLEE HAM & JENNIFER L. HOFFMAN, THE LINUX FOUND. & THE LAB'Y FOR INNOVATION SCI. AT HARV., REPORT ON THE 2020 FOSS CONTRIBUTOR SURVEY, https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/2020FOSSContributorSurveyReport_121020.pdf [https://perma.cc/6HLD-VSW9] (summarizing results of a survey among free/open source software ("FOSS") developers in 2020).

[108] *The 2021 State of the Octoverse*, GITHUB, https://octoverse.github.com/2021/ [https://perma.cc/QDW5-YC8Q].

[109] *Id.*

[110] *The Open Source Way 2.0*, OPEN SOURCE WAY 2.0 (Dec. 16, 2020), https://www.theopensourceway.org/the_open_source_way-guidebook-2.0.html [https://perma.cc/J6U8-YN9C].

[111] Shah & Nagle, *Why Do User Communities Matter for Strategy?*, *supra* note 67, at 5 ("Participants generally do not receive remuneration or other benefits from the community as a direct result of their work. Participants identify and choose the work they will undertake: the community does not assign tasks to participants, rather participants choose whether or not to participate and how to participate.").

wag the dog and the project is more likely to support the company's profits over the public's best interest.

b. Open Source's Support Structures

The degree to which projects are organized and supported vary. Some of the internet's most popular projects are supported by highly structured, well-funded organizations.[112] The Linux Foundation has over a thousand corporate members,[113] thousands of contributing developers, including many paid developers, and its net income in 2020 was $10,878,362.[114] Its organizational size is necessary to support its market share: nearly seventy-five percent of the internet's web servers run on Linux.[115] However, the wealth is not evenly spread in the community.[116] Contrast the Apache Software Foundation, which has thousands of contributors each year[117] organized around its flagship product, the Apache HTTP Server, that supports approximately one-third of the internet.[118] In 2019, the Apache Software Foundation's net income was negative $249,084.[119] Unlike Linux, its budget does not pay full-time developers; instead, Apache remains supported by a collective of volunteers.[120]

The inequitable and inefficient distribution of resources across the open-source community gives rise to security problems because insufficient resources

[112] Carlos Santos Jr., *Understanding Partnerships Between Corporations and the Open Source Community: A Research Gap*, 25 IEEE SOFTWARE 96, 96–97 (2008). But there is concern about corporate capture in that open-source projects begin to only serve the needs and preferences of their managers/funders. *See generally* Dahlander & Magnusson, *supra* note 92 (providing an example of published concerns about corporate-funded projects).

[113] *Members*, LINUX FOUND., https://www.linuxfoundation.org/our-members-are-our-superpower-2 [https://perma.cc/MPB2-U9BD].

[114] *The Linux Foundation*, PROPUBLICA, https://projects.propublica.org/nonprofits/organizations/460503801 [https://perma.cc/XYQ4-5RMM].

[115] *August 2019 Web Server Survey*, NETCRAFT (Aug. 15, 2019), https://news.netcraft.com/archives/2019/08/15/august-2019-web-server-survey.html [https://perma.cc/5G4K-FH7M].

[116] *See* NADIA EGHBAL, THE FORD FOUND., ROADS AND BRIDGES: THE UNSEEN LABOR BEHIND OUR DIGITAL INFRASTRUCTURE 59–65, https://www.fordfoundation.org/media/2976/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure.pdf [https://perma.cc/TLF9-YWDJ].

[117] Sally, *Apache in 2021—By the Digits*, APACHE SOFTWARE FOUND. BLOG (Jan. 3, 2022), https://blogs.apache.org/foundation/entry/apache-in-2021-by-the [https://perma.cc/QC3F-K3PX].

[118] *Usage Statistics of Apache*, W3TECHS, https://w3techs.com/technologies/details/ws-apache [https://perma.cc/UA4B-KPBX].

[119] *Full Text of "Full Filing" for Fiscal Year Ending April 2020*, PROPUBLICA, https://projects.propublica.org/nonprofits/organizations/470825376/202130539349300643/full [https://perma.cc/77SN-AAAC].

[120] *How the ASF Works*, APACHE SOFTWARE FOUND., https://www.apache.org/foundation/how-it-works.html [https://perma.cc/5DYN-JLBC].

mean insufficient developer support.[121] Without adequate developer support, bug reports will go unchecked, and code will go live unreviewed. Sometimes, it can take even a diligent, but overwhelmed maintainer years to respond to a pull request that patches a problem, simply because the volume of pull requests they get is untenable for a short-staffed project to keep up with.[122]

The 2014 Heartbleed incident is illustrative. The attack exploited a vulnerability in the OpenSSL library, which was maintained by four developers, only one of whom called it a full-time job.[123] These developers were solely responsible for over 500,000 lines of code, which at the time supported two-thirds of all websites, on a shoestring budget of $2,000 a year.[124] In the

[121] Eric Geller, *Lesson from Log4j: Open-Source Software Improvements Need Help from Feds*, POLITICO (Jan. 6, 2022, 3:15 PM), https://www.politico.com/news/2022/01/06/open source-software-help-526676 [https://perma.cc/37Q5-E4W9] [hereinafter Geller, *Lesson from Log4j*] (explaining that "Log4j and other similarly ubiquitous open source libraries often receive little dedicated scrutiny and maintenance, allowing flaws to remain hidden for long periods of time," because "while some foundations receive significant financial support from businesses that depend on open-source code . . . others operate on shoestring budgets").

[122] Nasif Imtiaz, Aniqa Khanom & Laurie Williams, *Open or Sneaky? Fast or Slow? Light or Heavy?: Investigating Security Releases of Open Source Packages*, IEEE TRANSACTIONS ON SOFTWARE ENG'G, June 9, 2022, at 1, 9 (concluding that study results show that one-fourth of open-source projects do not release the new version fixing a vulnerability until over twenty days after the fix was made); *see, e.g.*, SwiftOnSecurity, *Change Metasploit Alert Port from 444 to 4444*, GITHUB (Oct. 2, 2021), https://github.com/SwiftOnSecurity/sysmon-config/pull/105 [https://perma.cc/THG7-7U6H] (example of a pull request fixing an open-source project intended to improve system security pending for 1.5 years).

[123] While there were only four maintainers of the project, there were other intermittent contributors. Contributors, however helpful, do not carry out the same functions as maintainers and are not ultimately responsible for the health of the project. Nicole Perlroth, *Heartbleed Highlights a Contradiction in the Web*, N.Y. TIMES (Apr. 18, 2014), https://www.nytimes.com/2014/04/19/technology/heartbleed-highlights-a-contradiction-in-the-web.html [https://perma.cc/YHC3-MB42 (dark archive)] ("Most corporate OpenSSL users do not contribute money to the group, Mr. Marquess said. Google and Cisco say they contribute by encouraging their own engineers to look for bugs in the code while they are on the clock. The OpenSSL website shows that a Cisco engineer and several Google engineers have discovered bugs and created fixes over the years. A Google engineer, Neel Mehta, discovered the Heartbleed bug earlier this month, and two other Google engineers came up with the fix. Likewise, Microsoft and Facebook created the Internet Bug Bounty initiative, which pays engineers who responsibly disclose bugs in widely used systems like OpenSSL. The group paid Mr. Mehta $15,000 for his discovery — a windfall he donated to the Freedom of the Press Foundation. But open-source advocates say organizations that rely on the code should do more to help.").

[124] Julia Angwin, *The U.S. Government: Paying To Undermine Internet Security, Not To Fix It*, PROPUBLICA (Apr. 15, 2014, 12:50 PM), https://www.propublica.org/article/the-u.s.-government-paying-to-undermine-internet-security-not-to-fix-it [https://perma.cc/LQ4G-H545] (explaining that the maintainers of OpenSSL are dependent on "consulting gigs" to pay for their work); Perlroth, *supra* note 123 ("Over time, OpenSSL code has been picked up by companies like Amazon, Facebook, Netflix and Yahoo and used to secure the websites of government agencies like the F.B.I. and Canada's tax agency. It is baked into Pentagon weapons systems, devices like Android smartphones, Cisco desktop

aftermath of Heartbleed, experts found that the vulnerability was caused in no small part by "a major eyeball shortage"[125] and that there should have been at least six full-time maintainers to support the project.[126] Though they were short-staffed, the team of developers responded rapidly, developing and distributing a patch on the same day the vulnerability was disclosed.[127] In most circumstances, however, the public is unlikely to be so lucky.

The open-source community continues to struggle to resource some of the internet's most important projects.[128] Even after OpenSSL was attacked, little changed. As of 2021, the OpenSSL Software Foundation still only has two donors contributing $5,000 each, plus some crowdsourced donations.[129] One cryptographer noted that just $500,000 for projects like OpenSSL could have prevented events like Heartbleed.[130] More funding means more support. Volunteer developers have said they are more likely to contribute to a project if they are compensated fairly.[131]

Such pronounced resource gaps are less likely to persist with closed-source code, at least in theory. When a project grows, an organization can scale up investment to meet the demand for support, because if they do not maintain

phones and home Wi-Fi routers. Companies and government agencies could have used proprietary schemes to secure their systems, but OpenSSL gave them a free and, at least in theory, more secure option.").

[125] Edward W. Felten & Joshua A. Kroll, *Heartbleed Shows Government Must Lead on Internet Security*, SCI. AM. (July 1, 2014), https://www.scientificamerican.com/article/heartbleed-shows-government-must-lead-on-internet-security1/ [https://perma.cc/8NYM-4JLW].

[126] Angwin, *supra* note 124.

[127] Stephen Henson, *Add Heartbeat Extension Bounds Check*, GIT (Apr. 7, 2014), https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=96db9023b881d7cd9f379b0c154650d6c108e9a3 [https://perma.cc/97XU-VQ2D].

[128] *See* Owen Williams, *Open Source Developers, Who Work for Free, Are Discovering They Have Power*, TECHCRUNCH (Jan. 18, 2022, 12:50 PM), https://techcrunch.com/2022/01/18/open source-developers-who-work-for-free-are-discovering-they-have-power/ [https://perma.cc/8225-GUWN] (describing the power and labor dynamics for open source developers).

[129] Filippo Valsorda, *Professional Maintainers: A Wake-Up Call* (Dec. 11, 2021), https://words.filippo.io/professional-maintainers/ [https://perma.cc/9EQT-HQQY] ("GitHub Sponsors and Patreon are a nice way to show gratitude, but they are an extremely unserious compensation structure. The average maintainer of a successful project would qualify as a Senior Software Engineer, and those can easily make $150k–300k+/year. (90th percentile of SWE salaries, all levels: $355k in NYC, $232k in London, $163k in Berlin. Note that these are low-balls if you negotiate, especially in 2021/2022, and remote positions exist. Read some Patrick McKenzie.) When is the last time you've seen a GitHub Sponsors recipient making more than $1,000/month? That's *at least* 12 times less than the alternative.").

[130] *Heartbleed Bug: How Did It Happen, and How Do We Know It Won't Happen Again?*, JOHNS HOPKINS UNIV. (Apr. 10, 2014), https://hub.jhu.edu/2014/04/10/heartbleed-matthew-green/ [https://perma.cc/R8GS-5ANX] [hereinafter *Heartbleed Bug*].

[131] Chris Grams, *The Surprising Truth About How Many Developers Contribute to Open Source*, TIDELIFT (Dec. 10, 2019), https://blog.tidelift.com/the-surprising-truth-about-how-many-developers-contribute-to-open-source [https://perma.cc/ZLK5-BSB5].

the code, no one else will. The security of their products is tied to their reputation and brand; they are incentivized to fund their teams appropriately to outperform competitors. A commercial entity is also subject to contractual provisions—obligations to the customer they sold to, either explicit in the contract or implicit in the law governing sales and consumer protection. Poor security and defective products expose them to liability.[132]

Aside from the question of resources, project maintenance is also a question of interest and ability. A 2020 study reported that open-source developers spend on average 2.27% of their total contribution time on security "and express little desire to increase that time."[133] Popular projects need to be maintained, but the developer who built it for fun has no interest in taking on that responsibility.[134] Project maintenance is tedious, involving activities like sorting through hundreds of bug reports, most of which are unhelpful.[135] Without pay, it is unsurprising that the average developer spends a near-

[132] While technically defective open-source code contained in a commercial product or service can also give rise to liability, enforcement of that liability would require a customer to know the software contained open-source components, to attribute the harm to a defect in those open-source components, and to be able to bring that suit in court. In the case of open source, the current liability scheme has not proven successful. Trey Herr, Robert Morgus, Stewart Scott & Tianjiu Zuo, *Buying Down Risk: Cyber Liability*, ATL. COUNCIL (May 3, 2022), https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-liability/ [https://perma.cc/BF2G-58Y3] ("Without a clear negligence standard, applications of liability will remain patchwork, inconsistent, and opaque. This is the current state of software liability, despite continued calls for more significant financial incentives for more secure software development in the face of pressure to bring new features and services to market rapidly. The few suits brought against vendors have been settled out of court, preventing clear precedent and, crucially, avoiding clarity around a legal negligence standard.").

[133] *New Open Source Contributor Report from Linux Foundation and Harvard Identifies Motivations and Opportunities for Improving Software Security*, LINUX FOUND. (Dec. 8, 2020), https://www.linuxfoundation.org/press-release/new-open-source-contributor-report-from-linux-foundation-and-harvard-identifies-motivations-and-opportunities-for-improving-software-security/ [https://perma.cc/HW8X-LYWK]; *see also* Pattison-Gordon, *supra* note 77 ("There's a risk that the work that grabs volunteers' focuses isn't what's most important to safeguarding the ecosystem.").

[134] *See* dominictarr, *Statement on Event-Stream Compromise*, GITHUB, https://gist.github.com/dominictarr/9fd9c1024c94592bc7268d36b8d83b3a [https://perma.cc/A2RA-U7G2] [hereinafter dominictarr, *Statement on Event-Stream Compromise*] ("I didn't create this code for altruistic motivations, I created it *for fun*. I was learning, and learning is fun. . . . One time, I was working as a dishwasher in a restaurant, and I made the mistake of being too competent, and I got promoted to cook. This was only a 50 cents an hour pay rise, but massively more responsibility. It didn't really feel worth it. Writing a popular module like this is like that times a million, and the pay rise is zero."); Guido van Rossum, *Foreword for "Programming Python" in Programming Python (1st ed.)*, PYTHON, https://www.python.org/doc/essays/foreword/ [https://perma.cc/J6YD-LL4C] (demonstrating that Python, one of the most popular programming languages today, began as a pet project of a hobbyist).

[135] Jing Wang & John M. Carroll, *Behind Linus's Law: A Preliminary Analysis of Open Source Software Peer Review Practices in Mozilla and Python*, 2011 INT'L CONF. ON COLLABORATION TECHS. & SYS. 117, 117–24; Amy J. Ko & Parmit K. Chilana, *How Power Users Help and Hinder Open Bug Reporting*, CHI 2010 1665, 1665–74 (2010).

negligible amount of time on security.[136] Worse still, security maintenance is a thankless job. After the Log4Shell vulnerability was discovered, a few Apache volunteers worked tirelessly day and night on mitigation measures, releasing patches faster than most companies could have, all while being lambasted by the public for a problem they could not have prevented.[137] Even if open-source developers were perfectly motivated and supported, many of them are not security experts. As the Cyber Safety Review Board ("CSRB") report noted, software security demands a specific set of skills.[138] For closed-source code, a responsible company would hire a security professional.[139]

These circumstances are complicated by the fact that there is nowhere for an open-source project to go to die. Once a project takes off in popularity, the maintainer cannot take it offline without breaking all the third-party software built off it. They can simply walk away from the project, but doing so would allow pull requests to pile up, which, given the stigma around ignoring pull requests, would ultimately injure the maintainer's reputation.[140] And Git does not allow maintainers to disable pull requests without archiving the entire

[136] Valsorda, *supra* note 129 (explaining that security practices like two-factor authentication, mandatory code review, troubleshooting, quality standards, and a succession plan to ensure a project will not go unmaintained are impossible to demand without paying the maintainers); dominictarr, *Statement on Event-Stream Compromise*, *supra* note 134 (advocating for payment to maintainers).

[137] Volkan Yazici (@yazicivo), TWITTER (Dec. 10, 2021, 11:55 AM), https://twitter.com/yazicivo/status/1469349956880408583?s=20&t=FSP3a_p_2-dUvgZhN5s-fQ [https://perma.cc/SG45-VLYS] ("Log4j maintainers have been working sleeplessly on mitigation measures; fixes, docs, CVE, replies to inquiries, etc. Yet nothing is stopping people to bash us, for work we aren't paid for, for a feature we all dislike yet needed to keep due to backward compatibility concerns."); Pattison-Gordon, *supra* note 77 ("The vulnerability in open source software Log4J was detected and fixed faster than the similarly headline-topping vulnerability in SolarWinds' proprietary software . . . .").

[138] *See* CYBER SAFETY REV. BD., REVIEW OF THE DECEMBER 2021 LOG4J EVENT 25–26 (2022) [hereinafter CSRB LOG4J REPORT], https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf [https://perma.cc/HBW8-QGYL (staff-uploaded archive)] (proposing that the U.S. government and private sector companies invest in training and funding employees that can contribute to software security).

[139] Unfortunately, many do not. Security is seen as an expense, not an investment, and its benefits are hard to prove, because good security is the absence of an incident. Features, on the other hand, provide immediate, visible value and so companies often shortsightedly dedicate developer resources entirely to feature-development rather than security and maintenance. *Why Some Companies Don't Invest in Cybersecurity*, COLUMBIA MAG. (2015), https://magazine.columbia.edu/article/why-some-companies-dont-invest-cybersecurity [https://perma.cc/RD7M-GVUL] ("It's evident that some companies are choosing not to implement certain basic protections because they don't seem like necessary investments.").

[140] phendrenad2, Y HACKER NEWS (Jan. 28, 2021), https://news.ycombinator.com/item?id=25940799 [https://perma.cc/5N3L-AQWV].

project.[141] If, alternatively, a maintainer notifies users that they are stepping away from the project, then GitHub might send thousands of dependent repositories a "critical severity advisory" about it, further injuring the maintainer's reputation.[142] Often, a maintainer's best option is to transfer ownership to another willing maintainer, a form of collaboration and sharing core to the open-source ethos.[143] However, bad actors know and exploit this option, feigning genuine interest in maintaining a project with the actual intention of injecting malicious code as soon as they have control.[144]

To address these issues, solutions from corporate Contributing Consumers have cropped up. For example, RedHat profits by selling maintenance services to support Red Hat Linux, its open-source product forked from the original Linux kernel.[145] Companies that want to benefit from the cost-savings of open source but do not want to rely solely on the original open-source maintainer's diligence or maintain the project on their own will hire Red Hat to do it for them.[146] Google recently announced its new Assured Open Source Software service, which would provide Google Cloud customers with a similar service.[147] Both companies sell the guarantee of a reliable open-source project. In addition, Google has built a new team of developers, the Open Source Maintenance

[141] Iliana Etaoin, *There Is No "Software Supply Chain*,*"* (Sept. 19, 2022), https://iliana.fyi/blog/software-supply-chain/ [https://perma.cc/53VR-6BLN]; *Archiving Repositories*, GITHUB, https://docs.github.com/en/repositories/archiving-a-github-repository/archiving-repositories [https://perma.cc/C7D7-LS9A].

[142] Etaoin, *supra* note 141.

[143] dominictarr, *Statement on Event-Stream Compromise*, *supra* note 134 (describing how an experienced maintainer explained that he gave away the project "because it was easy to do so, and because sharing helps learning too," adding that "since the early days of node/npm, sharing commit access/publish rights, with other contributors was a widespread community practice").

[144] *Id.* (providing an explanation from an experienced maintainer that the bad actor's alleged good intentions were convincing: "I've shared publish rights with other people before . . . if I had realized they had a malicious intent I wouldn't have, but at the time it looked like someone who was actually trying to help me"). One user described how a bad actor took over his account: "[H]e emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and hav[e]n't for years." dominictarr, *I Don't Know What To Say*, GITHUB (Nov. 22, 2018), https://github.com/dominictarr/event-stream/issues/116 [https://perma.cc/B4B9-8X4H] [hereinafter dominictarr, *I Don't Know What To Say*].

[145] Josh Lerner & Jean Tirole, *Some Simple Economics of Open Source*, 50 J. INDUS. ECON. 197, 210 (2002).

[146] *Id.*

[147] Andy Chang, *Introducing Google Cloud's New Assured Open Source Software Service*, GOOGLE CLOUD (May 17, 2022), https://cloud.google.com/blog/products/identity-security/introducing-assured-open-source-software-service [https://perma.cc/3T4S-CENV]; Corin Faife, *Google Will Start Distributing a Security-Vetted Collection of Open-Source Software Libraries*, VERGE (May 17, 2022, 12:44 PM), https://www.theverge.com/2022/5/17/23097529/google-assured-open-source-software-security-vetted-libraries [https://perma.cc/T5X8-GAQP].

Crew, dedicated to helping maintainers of critical open-source projects improve security.[148]

These services promise to improve open-source security for the customers that pay, but the community has mixed feelings about the development.[149] Given open source's freedom-of-the-internet ethos, some members chafe against corporate involvement, which could lead to a decline in open-source contributions.[150] Several feel that companies profiting off open source is unethical.[151] By deleting seventeen lines of code to protest corporate pressure, one developer temporarily "broke the internet."[152] There are also concerns about corporate capture when companies become major funders.[153] While the elephant bears no malice towards the ant, corporate Contributing Consumers can have their blind spots; to expose them, open-source security efforts must involve the *whole* open-source community.

c. *Open Source's Weak Link*

Open source brings together a variety of constituents of the technology world—and its benefits and efficiencies do bring a net positive to society. Yet the security of the software remains a concern. This subsection delves into the how and why open source presents particular security worries.

Despite the responsible practices of Contributing Consumers, the open-source ecosystem remains vulnerable due to its Irresponsible Consumers—the *commercial* entities *profiting off* open source without contributing to its continued production or taking the basic security precautions that would prevent attacks

[148] Dennis Fisher, *New Google Team To Help Critical Open Source Projects Improve Security*, DECIPHER (May 12, 2022), https://duo.com/decipher/new-google-team-to-help-critical-open-source-projects-improve-security [https://perma.cc/ES5Y-W9H8].

[149] *See* Mathieu O'Neil, Laure Muselli, Mahin Rassi & Stefano Zacchiroli, *'Open Source Has Won and Lost the War': Legitimising Commercial—Communal Hybridisation in a F/OSS Project*, 23 NEW MEDIA & SOC'Y 1157, 1176–77 (2021).

[150] Denver Gingerich & Bradley M. Kuhn, *Give Up GitHub: The Time Has Come!*, SOFTWARE FREEDOM CONSERVANCY (June 30, 2022), https://sfconservancy.org/blog/2022/jun/30/give-up-github-launch/ [https://perma.cc/CZ3N-FSEX] ("We learned a valuable lesson that was a bit too easy to forget—especially when corporate involvement manipulates FOSS communities to its own ends."); Shah, *supra* note 101, at 1009–10 (describing how more corporate sponsorship of open-source contributions leads to a decline in the intrinsic motivation for volunteer developers to contribute).

[151] David Ramel, *Another Open Source Group Blasts GitHub Copilot, Advocates Leaving GitHub*, VISUAL STUDIO MAG. (July 1, 2022), https://visualstudiomagazine.com/articles/2022/07/01/leave-github.aspx [https://perma.cc/482R-YECW].

[152] Gallagher, *supra* note 46 (describing how a developer's frustration with corporate interference with his open-source project drove him to delete it, causing thousands of developers' code to fail).

[153] Martin Traverso, *Who Owns Open Source Projects? People or Companies?*, VENTUREBEAT (Aug. 27, 2021, 11:20 AM), https://venturebeat.com/2021/08/27/who-owns-open-source-projects-people-or-companies/ [https://perma.cc/SL2E-JTU6].

and alleviate some of the pressure on the open-source community.[154] These entities incorporate open-source code into products containing closed-source code and then use, sell, or license that product for profit. They take open-source code out of the ether and put it in front of users—selling a product whose integrity cannot be assured. There are often multiple Irresponsible Consumers in the supply chain—companies build and sell software components containing open source to each other, each adding new code, and potentially, new vulnerabilities every step of the way. Just as anyone can contribute to open source, anyone can use it, regardless of how irresponsible they are. And these Irresponsible Consumers contribute substantial risk.

Irresponsible Consumers fail to document open-source code they use at the point of integration. They hire developers to solve problems and open source offers a shortcut to delivering on expectations. Often, their developers are not required to get approval first, document the use, or review the code before incorporating it into their work.[155] This lackadaisical approach can lead to the incorporation of insecure code or an excessive amount of code into commercial software, increasing its risk surface. But, as long as the software works, the developer's job is done; Irresponsible Consumers reward new features above security checks. In this way, companies unwittingly grow to rely on undocumented open-source code.[156] If instead, that component was purchased from a third-party, then theoretically, the company's legal and procurement teams would be involved, the process would be heavily documented, a list of trusted vendors would be provided, and the product would be thoroughly vetted before acquisition.[157]

This failure to document open-source use is viral. Downstream customers of the Irresponsible Consumer who first integrated an open-source component without documentation are left in the dark. Today, twenty percent of the 5.1 million open-source components analyzed in an industry study do not contain

[154] While noncommercial entities may also be irresponsible, this Article focuses on commercial entities, because they pose the biggest threat.

[155] If there are requirements, they are generally ignored. Developers are evaluated on delivery of functionality. Companies, until very recently, have not had formal open-source policies and generally frowned on its use. It is easier to ask for forgiveness later, once the code is already deeply embedded with important systems relying on it. HENDRICK & MCKEAY, *supra* note 21, at 5 (reporting less than half of companies studied have a policy governing open-source development or usage); Matt Jacobs, *Open Source Licenses: No License, No Problem? Or . . . Not?*, SYNOPSYS (Sept. 23, 2020), https://www.synopsys.com/blogs/software-security/unlicensed-open-source-scenarios/ [https://perma.cc/MNB6-7L8A] (describing the ways in which corporate developers incorporate undocumented open-source code).

[156] *See* 2022 SYNOPSYS REPORT, *supra* note 16, at 16 (showing that developers fail to attach the appropriate open-source license to projects using open-source components, breaking the chain of documentation of its use in commercial software).

[157] Lokshin et al., *supra* note 75.

a valid open-source license.[158] Often, the original open-source project had a license; it got lost somewhere downstream once an Irresponsible Consumer got their hands on it. Without an accompanying license, any customer receiving software from an Irresponsible Consumer may never know they are using open source.

Irresponsible Consumers also regularly use un- or undermaintained projects.[159] If a project is not being updated, then chances are it is not being maintained and is therefore insecure. Irresponsible Consumers fail to track the frequency and quality of updates to a project. One study found that this results in eighty-eight percent of software used by the public containing open-source components from dormant projects, which means there are no eyeballs on a large portion of the code society relies on.[160] The security of undermaintained projects does not fare much better, but Irresponsible Consumers continue to use them as well. There is a famous comic in the software developer world that depicts "all modern digital infrastructure" resting on the back of an open-source project maintained by one developer in Nebraska.[161] Developers refer to this as the "bus factor," which is the number of project maintainers who, if hit by a bus and incapacitated, would cause that project to fail.[162] Projects with low bus factors are less likely to be secure.[163] Studies have found that *at least* twenty-three percent of all open-source projects have only one developer contributing code.[164] The rest are not much better; ninety-four percent of projects are kept alive by fewer than ten developers.[165]

Irresponsible Consumers also fail to scan for known and unknown vulnerabilities in the open-source code they use while building their products

[158] 2022 SYNOPSYS REPORT, *supra* note 16, at 16.

[159] PAUL ROSENZWEIG, STANFORD UNIV., CYBERSECURITY AND PUBLIC GOODS: THE PUBLIC/PRIVATE "PARTNERSHIP" 7–8 (2011) [hereinafter ROSENZWEIG, CYBERSECURITY AND PUBLIC GOODS]; ERIC BREWER, THE CONSEQUENCE OF SUCCESS: OSS IS CRITICAL INFRASTRUCTURE 7 (2022), https://docs.google.com/presentation/d/18hkLb6CIC49tBFp2nX4prbhKaUiHj_cfXPN95zg4dS0/edit#slide=id.p [https://perma.cc/A39H-7PQY] ("30% of packages have 1 maintainer, in practice many have zero . . . .").

[160] 2022 SYNOPSYS REPORT, *supra* note 16, at 19.

[161] *Dependency*, XKCD, https://xkcd.com/2347/ [https://perma.cc/L85B-92MQ].

[162] *Bus Factor*, CHAOSS, https://chaoss.community/metric-bus-factor/ [https://perma.cc/NX7H-4WLN].

[163] *Cf. coreinfrastructure*, GITHUB, https://github.com/coreinfrastructure/best-practices-badge [https://perma.cc/GBE7-7WPX] (requiring projects to have a bus factor of two or more, which means having at least two unassociated significant contributors, to obtain a gold badge for best practices).

[164] 2022 SYNOPSYS REPORT, *supra* note 16, at 20; *see also* lehors, *What Is "a Healthy Number" of Maintainers?*, GITHUB (May 9, 2022), https://github.com/ossf/tac/issues/101 [https://perma.cc/U9G6-5HRK] ("There have been 28 million npm package releases (this is all packages times all versions). Of all those releases, 16 million (that is not a typo, 16 with six zeroes) have one maintainer.").

[165] 2022 SYNOPSYS REPORT, *supra* note 16, at 19.

in the first instance.[166] Despite the catastrophic risk presented by Log4Shell, in the year following its discovery, at least a quarter of all *new* Log4j downloads pulled the old, vulnerable version—instead of decreasing over time, that percentage has stayed relatively constant.[167] Scanning at the point of integration could have notified the company that they are pulling a compromised version. Due to this failure to scan, Irresponsible Consumers continue to *actively* propagate software containing *critical* vulnerabilities upwards of fifteen years after they were discovered.[168]

They also fail to continue scanning their products for open-source vulnerabilities discovered after the software has been sold or implemented. The Log4Shell vulnerability illustrated the importance of multiple scans—it was not a known vulnerability when consumers first incorporated the code into their products. Only those who scanned again later had a chance to find it.[169] To demonstrate the pernicious threat of unscanned systems: one federal agency failed to find a vulnerable instance of Log4j, which permitted Iranian hackers to breach its systems and siphon data back to its own servers as early as February 2022. The agency did not even know it was breached until April 2022, when CISA conducted a proper vulnerability scan of its systems.[170] Without routine maintenance, vulnerabilities cannot be found and remediated.[171]

[166] PONEMON INST., COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE 6, https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf [https://perma.cc/K5HJ-HGEY] (finding that in 2019, forty-six percent of companies that suffered a data breach did not know they had a vulnerability in the first place, information which they could have learned through regular scans).

[167] *Log4j Exploit Updates*, SONATYPE, https://www.sonatype.com/resources/log4j-vulnerability-resource-center#latest-insights [https://perma.cc/L78A-BEKW].

[168] Sumeet Wadhwani, *15-Year-Old Python Vulnerability Still Affects Over 350,000 Open-Source Projects*, SPICEWORKS (Sept. 22, 2022), https://www.spiceworks.com/it-security/vulnerability-management/news/python-tarfile-extraction-vulnerability-software-supply-chain/ [https://perma.cc/PK9F-86MQ] ("This vulnerability's pervasiveness is furthered by industry tutorials and online materials propagating its incorrect usage. It's critical for developers to be educated on all layers of the technology stack to properly prevent the reintroduction of past attack surfaces.").

[169] *Apache Log4j Vulnerability Guidance*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Apr. 8, 2022), https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance [https://perma.cc/PHK2-3ZDS]; Google Cybersecurity Action Team, *Google Cloud Recommendations for Investigating and Responding to the Apache "Log4j 2" Vulnerability*, GOOGLE CLOUD BLOG (Dec. 13, 2021), https://cloud.google.com/blog/products/identity-security/recommendations-for-apache-log4j2-vulnerability [https://perma.cc/S5ZX-M485].

[170] Graham, *supra* note 9.

[171] BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 344 (2000) ("The only way to find security flaws in a piece of code is to evaluate it. That is true for all code, whether it is open source or proprietary. And you can't just have anyone evaluate the code, you need experts in security software evaluating the code. You need them evaluating it multiple times and from different angles, over the course of years.").

By failing to scan their own components, Irresponsible Consumers compound the deficient supply of "eyes" in the open-source ecosystem. Per Linus's law, open-source vulnerabilities can be found and mitigated before they are ever exploited—if there are enough developers looking. Without enough eyes on every important project, hackers have a greater opportunity to find vulnerabilities first. In July of 2022, the CSRB released its first report analyzing the Log4Shell incident and its implications.[172] The report concluded that "a focused review, performed by someone with sufficient experience with the security implications of adding the [vulnerable library], could have identified the unintended functionality (i.e., the vulnerability)."[173] The report added that "unfortunately, the resources to perform such a review were not available to the volunteer developers who led this open-source project in 2013," when the vulnerability was first introduced.[174]

In addition to scanning, companies must also deploy patches in a timely fashion. As discussed earlier, open disclosure also reduces the time between when a bug is found and when users are given the chance to fix it. This theoretically gives developers a head start, but many fail to take advantage of the opportunity, either because of recklessness or ignorance. A study found that eighty-five percent of software analyzed contained components that were outdated more than four years—meaning that the company either chose to download an old, vulnerable version of a component or failed to apply an available patch for a known vulnerability.[175] On average, software programs have five *unpatched* high-risk or critical vulnerabilities.[176] In those instances, the code's openness gives the advantage to hackers, who are free to exploit the publicly disclosed bug in unpatched systems.

Irresponsible Consumers fail to do the bare minimum for security: using patches *provided by others*. Even when provided with a patch, Irresponsible Consumers do not distribute it to customers,[177] because they cannot be bothered to assess whether the vulnerability actually affects their products.[178] Not all vulnerabilities in an open-source library require urgent fixes, but some do.

[172] Paul Rosenzweig, *The First Cyber Safety Review Board Report Is Out*, LAWFARE (July 14, 2022, 3:35 PM), https://www.lawfareblog.com/first-cyber-safety-review-board-report-out [https://perma.cc/9ABN-GMP2] [hereinafter Rosenzweig, *The First Cyber Safety Review*].

[173] *Id.*

[174] *Id.*

[175] 2022 SYNOPSYS REPORT, *supra* note 16, at 19.

[176] HENDRICK & MCKEAY, *supra* note 21, at 2, 15.

[177] REID ET AL., *supra* note 71, at 10 (stating the results of a study that found that even when a patch was provided to maintainers only a small percentage published the patch).

[178] *See* Serena Elisa Ponta, Henrik Plate & Antonino Sabetta, *Beyond Metadata: Code-Centric and Usage-Based Analysis of Known Vulnerabilities in Open-Source Software*, *in* 2018 IEEE INTERNATIONAL CONFERENCE ON SOFTWARE MAINTENANCE AND EVOLUTION 449, 459 (2018), https://arxiv.org/pdf/1806.05893.pdf [https://perma.cc/UA35-RRWL].

Irresponsible Consumers avoid this analysis and instead wait for evidence their products were impacted before issuing a patch to customers. For example, nearly two weeks after the Log4Shell vulnerability was identified, thirty percent of organizations had not even begun to look for the bug in their systems, exposing millions of end-users to the effects of potential exploits.[179] Nearly half a year later, researchers found that sixty percent of the hundreds of millions of devices affected by the Log4Shell vulnerability remained unpatched.[180]

The enormity of open source's attack surface demands that its vulnerabilities should be addressed first, yet Irresponsible Consumers are not addressing them at all.[181] They do not apply the same care to open source as they would to their closed-source code, because they lack the incentives. Open source offers them no intellectual property value, is not tied to their brand, and is not governed by contracts. Because they do not see open-source code as a valuable asset to protect, they do not subject it to the same mandatory procurement processes or rigorous development standards.[182] Finally, because open-source software is built and used by other people, its maintenance is shrugged off as someone else's problem. Irresponsible Consumers aim to distribute open source "as-is" (indeed, the open-source license distributes the component "as-is") and they resist any accountability for it.[183]

Admittedly, commercial incentives have not been sufficient to fully secure closed-source code.[184] Companies still see security as a pesky expense taking developer time away from profitable value creation. Executives undervalue the

[179] Yoran, *supra* note 3.

[180] PERKAL, *supra* note 31, at 2; Newman, *Log4j Vulnerability*, *supra* note 31 (stating that Log4J impacted hundreds of millions of devices).

[181] Eileen Yu, *Open Source Security Needs Automation as Usage Climbs Amongst Organisations*, ZDNET (July 17, 2022), https://www.zdnet.com/article/open source-security-needs-automation-as-usage-climbs-amongst-organisations/ [https://perma.cc/W6D8-SF83] [hereinafter Yu, *Open Source Security Needs Automation*] (quoting expert saying that "tapping open source meant that any vulnerability in the codes then could be inherited by the host enterprise application" and "[o]pen source vulnerabilities, hence, always should be addressed first").

[182] 2022 SYNOPSYS REPORT, *supra* note 16, at 16–17; *see also* Lokshin et al., *supra* note 75.

[183] Frank Nagle, *Open Source and Firm Productivity*, 65 MGMT. SCI. 1191, 1194 (2018) [hereinafter Nagle, *OS & Productivity*] ("Perhaps the most concerning risk of all is the lack of a contractual relationship between a firm using non-pecuniary OSS and any one entity responsible for the development of such software, which leaves the firm with no one to sue when something goes wrong."); *see also* Sherwin Rosen, *Transaction Costs and Internal Labor Markets*, 4 J.L. ECON. & ORG. 49, 53–54 (1988) (theorizing that shared ownership of assets is inefficient because an "exceedingly complicated contractual system" is required to make each individual do their share).

[184] David E. Sanger, Nicole Perlroth & Julian E. Barnes, *As Understanding of Russian Hacking Grows, So Does Alarm*, N.Y. TIMES (May 28, 2021), https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html [https://perma.cc/5W9Z-QUJT (staff-uploaded, dark archive)] ("SolarWinds, the company that the hackers used as a conduit for their attacks, had a history of lackluster security for its products, making it an easy target, according to current and former employees and government investigators.").

importance of investing in secure development practices and consumers undervalue security as a factor in choosing a vendor.[185] Security is unobservable; it can only be disproven, not proven, because good security means the absence of an incident. This dynamic can make it easier for Irresponsible Consumers to hide flaws than to actually fix them. Even when consumers demand observable security measures, such as encryption, they are often not the most impactful measures. These factors account for the relatively poor security posture of software across the board, including open source. But open source lacks even the theoretical incentives that spur investment in closed-source code.

3. Licenses Governing Open Source

Open source is a technology and a community, and it is also a license that confers largely unenforceable property rights.[186] Code is an information-based good, which means its value is intangible.[187] With informational goods, property rights are conferred and protected by intellectual property law.[188] Owning the copyrights to software means being able to restrict access and use to it. Open source, though copyrighted in theory, expressly foregoes the right to exclude access to its code.

When developers write code on the company's dime, the code constitutes a valuable asset, increasing the company's worth. When licensing these assets, many companies deliver the software in binary code to obscure the copyrighted source code.[189] The code's property value is directly tied to its license's enforceability. A company cannot sell software if it is widely available for free—they have significant incentive to proactively enforce licenses.

Open-source software, on the other hand, is distributed via open-source licenses.[190] Open-source licenses protect the right to distribute over the right to

[185] *Heartbleed Bug*, *supra* note 130.

[186] Swire, *A Theory of Disclosure for Security and Competitive Reasons*, *supra* note 68, at 1353 ("Open Source software not only lacks technical protection against competition and disclosure, but it lacks traditional legal protections.").

[187] *See* BLIND ET AL., *supra* note 28, at 34.

[188] *See, e.g.*, U.S. COPYRIGHT OFF., COPYRIGHT REGISTRATION OF COMPUTER PROGRAMS, CIRCULAR 61, https://www.copyright.gov/circs/circ61.pdf [https://perma.cc/L8H7-DHHJ (staff-uploaded archive)] (explaining the copyright protections afforded to software).

[189] Christian H. Nadan, *Open Source Licensing: Virus or Virtue?*, 10 TEX. INTELL. PROP. L.J. 349, 350–51 (2002) (describing how proprietary software is almost always distributed in binary form to protect intellectual property and prevent misappropriation).

[190] David McGowan, *Legal Implications of Open-Source Software*, 2001 U. ILL. L. REV. 241, 253–54.

exclude.[191] Although the specific nature of these licenses can differ slightly,[192] they all decidedly surrender rights traditionally tied to property ownership and are largely unenforceable even for the rights they do preserve.[193] Closed-source code licenses tend to come with contractual obligations, such as restrictions on how the code can be used, how long it can be used for, whether it can be provided to others, and what, if any, requirements are on the user of the software—use of the code is conditional on compliance. Comparatively, open-source licenses impose very few restrictions. Technically, violating an open-source license can constitute a breach of contract and copyright infringement.[194] In practice, enforcement is expensive, and developers stand to gain very little from it.[195]

Resolution of the open-source security problem cannot hang its hat on adding fees, conditions, or restrictions to licenses to curb excessive or irresponsible use of a project. Open source's licenses reflect the community's ethos; any changes would compromise what makes the code open.

[191] STEVEN WEBER, THE SUCCESS OF OPEN SOURCE 1 (2004).

[192] Copyleft licenses require that any product built with the licensed code must also be open-sourced under a copyleft license. RICHARD STALLMAN, *What Is Copyleft?*, *in* FREE SOFTWARE, FREE SOCIETY: SELECTED ESSAYS OF RICHARD M. STALLMAN 91, 91–92 (Joshua Gay ed., 2002); Michael J. Madison, *Reconstructing the Software License*, 35 LOY. U. CHI. L.J. 275, 283–84 (2003). Permissive licenses are true to their name: they allow users of the licensed open-source project to incorporate the code into a proprietary product and profit off it. LAWRENCE ROSEN, OPEN SOURCE LICENSING: SOFTWARE FREEDOM AND INTELLECTUAL PROPERTY LAW 69–70 (2005). There is an ongoing legal and philosophical debate about the differences between free software and open-source software. Richard Stallman, *Why Open Source Misses the Point of Free Software*, GNU OPERATING SYS., https://www.gnu.org/philosophy/-misses-the-point.en.html [https://perma.cc/5X8H-LYS6] ("For the free software movement, free software is an ethical imperative, essential respect for the users' freedom. By contrast, the philosophy of open source considers issues in terms of how to make software 'better'—in a practical sense only. It says that nonfree software is an inferior solution to the practical problem at hand.").

[193] *See* LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 265 (2004); *see also* Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369, 446 (2002) (arguing that the copyright-based licensing of OSS is used "only as a form of institutional jiujitsu to defend from intellectual property" and suggesting that "[a] complete absence of property in the software domain would be at least as congenial to free software development as the condition where property exists, but copyright permits free software projects to use licensing to defend themselves from defection").

[194] *See* Jacobsen v. Katzer, 535 F.3d 1373, 1381–82 (Fed. Cir. 2008).

[195] Some nonprofits bring actions on behalf of the developer community, such as the Software Freedom Conservancy, but they are rarely successful. *See Conservancy's Copyleft Compliance Projects*, SOFTWARE FREEDOM CONSERVANCY, https://sfconservancy.org/copyleft-compliance/ [https://perma.cc/DUE8-GMXT]. Other organizations focus on raising awareness of license conditions and encouraging compliance. GPL-VIOLATIONS.ORG PROJECT, http://gpl-violations.org/ [https://perma.cc/WV3X-S2WD] ("The ultimate goal is to make companies engaging in the distribution of products based on GPL licensed software understand that GPL is not public domain, and that there are license conditions that are to be fulfilled.").

B. *Consequences of Open Source's Unique Structure*

Given open source's unparalleled value proposition, it is unsurprising that it is now being used by everyone, everywhere. It bears the qualities of a public good and is as indispensable as national highways. It is at the core of our most critical infrastructure systems. Because society's most essential functions rely on open source, its vulnerabilities present a security threat to our critical infrastructure.

1. Open Source Is Everywhere

Today, the public and private sectors see the promise of open source and they are using it more than ever. Almost all modern commercial software is "built on hundreds of small, distributed free and open-source software libraries owned and maintained in different ways."[196] International "market leaders such as Google, IBM, Microsoft, SAP, and Siemens as well as many small companies" realize the promise of open source and incorporate it heavily into their development.[197] Ford, Walmart, and numerous other nontechnology companies are also big users of open-source software.[198] Corporations and academic institutions are setting up open-source program offices to coordinate the use of open source[199] and the U.S. Department of Defense ("DoD") uses enough open source that a formal policy was designed permitting use and

[196] SASHA ROMANOSKY, JOHN BORDEAUX, MICHAEL J.D. VERMEER, JONATHAN W. WELBURN, AARON STRONG & ZEV WINKELMAN, HOMELAND SEC. OPERATIONAL ANALYSIS CTR., IDENTIFYING CRITICAL IT PRODUCTS AND SERVICES xi (2022), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA900/RRA923-2/RAND_RRA923-2.pdf [https://perma.cc/4XXB-Z8FY]. *See generally* Andrea Bonaccorsi, Silvia Giannangeli & Cristina Rossi, *Entry Strategies Under Competing Standards: Hybrid Business Models in the Open Source Software Industry*, 52 MGMT. SCI. 1085 (2006) (addressing different strategies used by software firms that utilize open source).

[197] Christof Ebert, *Guest Editor's Introduction: How Open Source Tools Can Benefit Industry*, 6 IEEE SOFTWARE 50, 50–51 (2009); Perlroth, *supra* note 123 ("Much of the invisible backbone of websites from Google to Amazon to the Federal Bureau of Investigation was built by volunteer programmers in what is known as the open source community.").

[198] TJ McCue, *Ford Motor Company Sees Open Source*, FORBES (Jan. 10, 2013, 5:27 PM), https://www.forbes.com/sites/tjmccue/2013/01/10/ford-motor-company-sees-open-source/?sh=42c7251cacff [https://perma.cc/U7UT-SV5W]; Simon Phipps, *Walmart's Investment in Open Source Isn't Cheap*, INFOWORLD (Aug. 22, 2014, 6:00 AM), https://www.infoworld.com/article/2608897/walmart-s-investment-in-open-source-isn-t-cheap.html [https://perma.cc/8C2H-NQ3A].

[199] FOSSA Editorial Team, *Building an Open Source Program Office*, FOSSA (Mar. 8, 2021), https://fossa.com/blog/building-open-source-program-office-ospo/ [https://perma.cc/L5DU-6UVB] ("Microsoft, Google, Twitter, and Netflix are just a few examples of global enterprises that have Open Source Program Offices."); Todo Group & Ospology, *Academic OSPOs: Fostering Open Source Culture at Universities*, LINUX FOUND. (Nov. 17, 2021, 8:00 AM), https://community.linuxfoundation.org/events/details/lfhq-todo-group-presents-academic-ospos-fostering-open-source-culture-at-universities/ [https://perma.cc/38EZ-XJRY].

contribution.[200] Open source is driving innovation through entrepreneurship by allowing "small start-ups to have a large impact, even when they are capital constrained, due to the nonpecuniary, or free, nature of these critical inputs."[201] For example, WhatsApp, which was acquired in 2014 by Meta for nineteen billion dollars, was built on the back of open-source software.[202]

This has led to meteoric growth in the volume of open-source code in the public-facing ecosystem. Within four years, the average number of open-source components per commercial application jumped from 84 to 528.[203] These developments have led one member of Congress to conclude, "It's safe to say that anyone who has used a computer has relied on open source software."[204]

Not all open-source projects are equally critical to society. While text-generated artificial intelligence art might be astonishing and amusing, our day-to-day safety and security do not rely on it. This Article's focus is on the open-source projects and support systems that enable the country's most important systems and networks to function.

2. Open Source Has Become Critical Infrastructure

CISA defines critical infrastructure as functions and assets "so vital to the United States that [their] incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety."[205] Open source fits the bill. As an asset, the most important open-source libraries resemble semiconductors in the essential functionality they provide to multiple critical infrastructure sectors. As a sector, open source resembles national defense as an ecosystem of components working collectively and continuously to protect and defend the public. As a function, open-source maintenance

[200] Chief Information Officer, *DoD Open Source Software FAQ*, U.S. DEP'T DEF. (Oct. 28, 2021), https://dodcio.defense.gov/open-source-software-faq/ [https://perma.cc/4AS3-QT4B].

[201] Nagle, *OS & Productivity*, *supra* note 183, at 1191; *see also* Christof Ebert, *A Brief History of Software Technology*, 25 IEEE SOFTWARE 22, 23 (2008); Christof Ebert, *Open Source Drives Innovation*, 24 IEEE SOFTWARE 105, 108 (2007).

[202] *WhatsApp Open Source*, WHATSAPP, https://web.archive.org/web/20160304091651/http://www.whatsapp.com/opensource/ [https://perma.cc/UVQ9-LFH6].

[203] Danny Bradbury, *When Software Depends on a Project Thanklessly Maintained by a Random Guy in Nebraska, Is Open Source Sustainable?*, REG. (May 10, 2021, 10:45 AM), https://www.theregister.com/2021/05/10/untangling_open_sources_sustainability_problem/ [https://perma.cc/7WW3-9XXU]. *See generally* GORDON HAFF, REDHAT, THE STATE OF ENTERPRISE OPEN SOURCE (2022) [hereinafter STATE OF OS], https://www.redhat.com/en/resources/state-of-enterprise-open-source-report-2022 [https://perma.cc/6U92-JBBD (staff-uploaded archive)] (discussing survey responses from IT leaders about open source and its growth).

[204] Pattison-Gordon, *supra* note 77 (quoting Rep. Bill Foster, D-Ill).

[205] *Infrastructure Security*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/infrastructure-security [https://perma.cc/P9LE-NBYJ].

resembles the product supply chain as support infrastructure integral to the delivery of services.

Critical infrastructure relies on open source to function. CISA identified sixteen critical infrastructure sectors, many of which support each other.[206] It also identified Section 9 entities, the most important entities within these sectors.[207] Finally, it identified fifty-five National Critical Functions, nearly all of which span multiple critical infrastructure sectors.[208] For example, "maintain[ing] access to medical records" is a National Critical Function, which falls neatly under the Healthcare and Public Health Sector, but also implicates the Communications, Energy, Information Technology, and Manufacturing Sector.[209] Open source enables all of this critical infrastructure, providing value behind the scenes to ensure our power grid, hospitals, wastewater management systems, and nuclear systems continue to function.[210] The open-source project running on a power generator is as important to the delivery of electricity as the generator itself.[211]

[206] *Critical Infrastructure Sector*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/critical-infrastructure-sectors [https://perma.cc/926T-STYQ]. These sectors include the chemical sector, communications sector, dams sector, emergency services sector, financial services sector, government facilities sector, information technology sector, transportation systems sector, commercial facilities sector, critical manufacturing sector, defense industrial base sector, energy sector, food and agriculture sector, healthcare and public health sector, nuclear reactors, materials and waste sector, and water and wastewater systems. *Id.*

[207] Exec. Order No. 13,636, 78 Fed. Reg. 11739, 11742 (Feb. 12, 2013) (designating certain entities, considered most important in their sectors, as Section 9 entities). Section 9 entities are defined as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." *Presidential Executive Order (EO) 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure Support to Critical Infrastructure at Greatest Risk ("Section 9 Report") Summary*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (May 8, 2018), https://www.cisa.gov/sites/default/files/publications/EO-13800-Section-9-Report-Summary-20180508-508.pdf [https://perma.cc/3s79-NE4E (staff-uploaded archive)].

[208] National Critical Functions are broken into four function categories: Connect, Distribute, Manage, and Supply. Some of the functions identified as critical include providing internet-based content, information, and communications services; distributing electricity; maintaining access to medical records; and providing information technology products and services. *Status Update on the National Critical Functions*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Dec. 15, 2021) [hereinafter CISA, *Status Update Memo*], https://www.cisa.gov/sites/default/files/publications/2021_ncf-status_update_508.pdf [https://perma.cc/DWG8-TXZK].

[209] DEP'T OF HEALTH AND HUM. SERVS., PUBLIC HEALTH AND SOCIAL SERVICES EMERGENCY FUND: JUSTIFICATION OF ESTIMATES FOR APPROPRIATIONS COMMITTEE 93 (2022), https://www.hhs.gov/sites/default/files/fy-2022-phssef-cj.pdf [https://perma.cc/9EM6-WBVC (staff-uploaded archive)].

[210] 2022 SYNOPSYS REPORT, *supra* note 16, at 6–8.

[211] Dan Assaf, *Government Intervention in Information Infrastructure Protection*, *in* 253 CRITICAL INFRASTRUCTURE PROTECTION 29, 34 (Eric Goetz & Sujeet Shenoi eds., 2008).

Open source is present in the technology of every critical infrastructure sector. A 2022 report discovered that 100% of software from the computer hardware and semiconductor industry, the cybersecurity industry, the energy and clean tech industry, and the internet-of-things industry contained some amount of open-source code upon review.[212] Of the codebases scanned in the internet and software infrastructure industry, 98% contained open-source code.[213] Of the codebases scanned in the transportation industry, the financial services industry, and the manufacturing industry, 97% contained open-source code.[214] Of the codebases scanned in the telecommunications industry, 95% contained open-source code, and of the codebases scanned in the healthcare industry, 93% contained open-source code.[215] Over 90% of *every* critical infrastructure sector's software contains open-source code.[216] And it is a substantial amount of code. For example, 60% of the total code used by the transportation industry and a whopping 80% of the total code used by the internet sector was open source.[217]

This has not gone unnoticed. A January 2022 White House briefing statement described software as "ubiquitous across every sector of our economy and foundational to the products and services Americans use every day. Most major software packages include open source software . . . [which] brings unique value but has unique security challenges."[218] The Biden administration also recognizes that beyond its ubiquity, software, and specifically open source, is integral to the government's capacity to serve the public. A 2021 executive order, which came months before the Log4Shell vulnerability was discovered, states that the "security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions."[219] This holds as true for private sector critical infrastructure as it does for government systems.

Existing open-source critical infrastructure includes two types of projects. First, it includes projects that rank among the most popular on the internet—a measure that cannot be captured by the number of downloads alone.[220]

[212] 2022 SYNOPSYS REPORT, *supra* note 16, at 8.

[213] *Id.*

[214] *Id.*

[215] *Id.*

[216] *See id.*

[217] *Id.* at 12.

[218] *Readout of White House Meeting on Software Security*, WHITE HOUSE (Jan. 13, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/ [https://perma.cc/3BQ8-GJ9C].

[219] Exec. Order No. 14,028, 86 Fed. Reg. 26633, 26637 (May 12, 2021).

[220] For instance, traffic is another metric that can gauge popularity, as are other insights such as shares and conversation on social media platforms.

Exploitations of these projects can have wide-reaching effects that are hard to anticipate; part of the fear in Log4Shell's fallout was the uncertainty as to where an exploit might hit next and what it might take offline. The Log4j library's ubiquity was only discovered after its exploit; knowledge of its popularity, even as a passive dependency, could have raised awareness as to its criticality.[221] Second, it includes projects, regardless of the volume of direct users, that our National Critical Functions depend on. An open-source project is critical infrastructure even if only one wastewater management company's core functions rely on it.

Open source is more than just discrete projects supporting infrastructure; it is the community behind the projects. The critical infrastructure regulatory regime does not focus entirely on assets, or in this case, specific projects—it recognizes that a sector maintaining the infrastructure is as critical as the assets they generate.[222] In the 2014 Quadrennial Homeland Security Review ("QHSR"), the government explicitly recognized aging and neglect of critical systems and assets as threats to critical infrastructure.[223] The report cites the Deepwater Horizon oil spill as an example of poor maintenance of a critical infrastructure asset that caused devastating effects.[224] Whether the cause is a bad actor, a natural disaster, or wear and tear, critical infrastructure assets are constantly under threat and their maintenance must be financially supported. Open source is no different. To remain reliable, a project must be regularly evaluated, fortified, and improved to secure it against aging and attack, which makes the open-source community critical infrastructure as well.

Just as much of existing critical infrastructure is owned by the private sector, much of open-source infrastructure is controlled by the open-source

[221] *See* Kyle Alspach, *'Less Obvious' Uses of Log4j Pose a Major Risk*, VENTUREBEAT (Dec. 13, 2021), https://venturebeat.com/security/less-obvious-uses-of-log4j-pose-a-major-risk/ [https://perma.cc/7WjZ-H3ZK] (reporting that internal research from a security company shows that more than eighty-nine percent of all environments have vulnerable Log4j libraries but that "in many of them, the dev teams are sure they have zero exposure" and are surprised to learn one of their software components uses Log4j).

[222] Indeed, CISA already identifies "Maintain Supply Chains" as a National Critical Function. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., NATIONAL CRITICAL FUNCTIONS: STATUS UPDATE TO THE CRITICAL INFRASTRUCTURE COMMUNITY 3 (2020), https://www.cisa.gov/sites/default/files/publications/ncf-status-update-to-critical-infrastructure-community_508.pdf [https://perma.cc/G5NV-K6CH]. The software supply chain is just as critical as physical supply chains.

[223] *See* U.S. DEP'T OF HOMELAND SEC., THE 2014 QUADRENNIAL HOMELAND SECURITY REVIEW 5 (2014), https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf [https://perma.cc/ZR65-PL2M].

[224] The 2014 QHSR cited the 2010 Deepwater Horizon oil spill—an industrial accident caused in part by negligence—as a homeland security hazard. *See id.*

community supporting it.[225] Open source cannot be secured by the government or owners and operators of critical infrastructure assets that use open source; open-source security must involve the open-source community. The Obama administration recognized that "[c]ritical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient."[226] Ultimately, the open-source community, including its direct consumers, must "bear primary and substantial responsibility for addressing the public safety risks posed by their industries."[227]

Not only is the open-source community uniquely positioned to support existing uses of open source in critical infrastructure, but it is also uniquely positioned to develop contingency plans to substitute existing projects and produce new assets for future use.[228] Projects in high demand today may lose favor tomorrow and otherwise nascent projects might gain substantial traction. We have seen this in other critical infrastructure sectors. Where cloud servers were once considered fringe technology, today the government has invested billions in cloud computing, making it new critical infrastructure.[229] This is important. Relatively unpopular or unimportant projects today can serve society during a crisis in ways that are hard to foresee now. The value of treating an ecosystem as critical infrastructure is that it avoids missing the forest for the trees.

[225] Many policy documents claim eighty-five percent of critical infrastructure ("CI") is privately owned. *See* Christopher Bellavita, *How Proverbs Damage Homeland Security*, HOMELAND SEC. AFFS., Sept. 2011, at 1, 1. The actual percentage has never been empirically established, and in any case, would vary widely depending on how CI is defined and identified. *See id.* at 1–2.

[226] THE WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE 1 (2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.cc/RCH8-R5M6 (staff-uploaded archive)].

[227] OFF. OF HOMELAND SEC., NATIONAL STRATEGY FOR HOMELAND SECURITY 33 (2002), https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf [https://perma.cc/65GN-YA92].

[228] *See Homeland Infrastructure Foundation-Level Data*, U.S. DEP'T HOMELAND SEC., https://gii.dhs.gov/hifld/content/about-hifld [https://perma.cc/T5UE-FDYH] [hereinafter DHS, *HIFLD*]. The major CI interagency database using the capabilities approach is known as Homeland Infrastructure Foundation-Level Data. Four lead agencies—DHS, DoD, the National Geospatial-Intelligence Agency, and the U.S. Geological Survey—compile data gleaned from outreach to public and private sector partners. *Id.*

[229] *See* Chris Cornillie, *This Is IT: Federal Cloud Spending To Top $8 Billion in FY 2021*, BLOOMBERG L. (Aug. 20, 2021, 7:05 AM), https://news.bloomberglaw.com/tech-and-telecom-law/this-is-it-federal-cloud-spending-to-top-8-billion-in-fy-2021 [https://perma.cc/A34W-NT97 (staff-uploaded, dark archive)].

3. Open Source's Security Issue Is a Critical Infrastructure Security Issue

Open source is the keystone to our critical infrastructure; without it, our most important systems would collapse. This makes open-source security a matter of critical infrastructure security. Each of the critical infrastructure sectors and assets are key to delivery of National Critical Functions.[230] Indeed, the open-source supply chain is arguably a National Critical Function itself.[231] A threat to one link in the chain threatens to incapacitate the whole function.[232]

The risk of collapse is far from hypothetical. A study found that forty to sixty percent of the codebases analyzed in critical infrastructure sectors contain open-source vulnerabilities.[233] That means nearly half of the systems society relies on for its safety and productivity are susceptible to attack. And, as Log4Shell demonstrated, it only takes one bug in a small, popular, yet rarely used open-source library to take down a whole network. Critical infrastructure sectors and functions cannot be protected without improving open-source security.

Given its benefits, the solution is not to move away from open source. In any event, it would be impractical, and perhaps impossible, to do so. It is too embedded in our systems, and the cost of replacing every open-source component with secure, newly developed closed-source code would be prohibitively expensive and, given the poor state of commercial software

[230] *See generally* ORG. FOR ECON. COOP. & DEV., OECD REVIEWS OF RISK MANAGEMENT POLICIES: GOOD GOVERNANCE FOR CRITICAL INFRASTRUCTURE RESILIENCE (2019), https://www.oecd.org/gov/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm [https://perma.cc/RA8A-GPGU] (exploring critical infrastructure and proposing policies to increase resilience with critical infrastructure).

[231] CISA, *Status Update Memo*, *supra* note 208 (identifying "Maintain Supply Chain" as a National Critical Function).

[232] Academics call the possibility of a single event triggering widespread failures and negative effects spanning multiple organizations, sectors, and nations a "systemic risk." CHRISTOPHER WILSON, TAMAS GAIDOSCH, FRANK ADELMANN & ANASTASIIA MOROZOVA, INT'L MONETARY FUND, CYBERSECURITY RISK SUPERVISION 9 (2019), https://www.imf.org/-/media/Files/Publications/DP/2019/English/CRSEA.ashx [https://perma.cc/PZ6A-3T24 (staff-uploaded archive)]. *See generally* Pawel Smaga, *The Concept of Systemic Risk*, 5 SYSTEMIC RISK CTR. 1 (2014) (discussing the concept of systemic risk and the vulnerabilities that can lead to it).

[233] 2022 SYNOPSYS REPORT, *supra* note 16, at 12.

security, may not solve the fundamental issue.[234] The issue is not the code[235]: it is the lack of institutions securing the code.

II. OPEN SOURCE'S SECURITY PROBLEM DERIVES FROM ITS PUBLIC GOOD FEATURES

Identifying the ways in which open source resembles a public good can elucidate the root cause of its security problem. Section A of this part will describe open source's public good characteristics. Section B will address how, like most public goods, open source is susceptible to certain market failures. These market failures manifest as a free-rider problem in that users of open source do not contribute to its production or maintenance; negative externalities, in that open-source security issues impact innocent third parties; and asymmetric information, in that its decentralized and informal distribution channels obscure relevant information. Section C will review the consequences of these market failures: a tragedy of the commons that the least-cost avoider will not resolve. Analyzing these issues shows that incentives are at the root of the problem.

A. *Open Source Is an (Impure) Public Good*

Public goods have been described as "irreducible elements of each public economy."[236] They can be privately provisioned, such as most public health

[234] *See* Joan Engebretson, *FCC Attempts To Explain Rip-and-Replace Shortfall: Large Carriers Could Get Squeezed Out*, TELECOMPETITOR (Feb. 9, 2022, 4:21 PM), https://www.telecompetitor.com/fcc-attempts-to-explain-rip-and-replace-shortfall-large-carriers-could-get-squeezed-out/ [https://perma.cc/VEA3-TUQA]. Huawei technology is not nearly as pervasive in the country as open source is, yet the government's attempt to replace all Huawei components with more secure parts is going to cost billions more than was originally allocated for it. *Id.* Software components are also difficult to replace wholesale. In today's complex software ecosystem, components are no longer purely independent of each other and perfectly modular. Software has long chains of dependencies and so replacing one component can have unanticipated effects on other components, threatening the overall functionality or integrity of the system. Replacing software can be just as costly.

[235] *See generally* STATE OF OS, *supra* note 203 (demonstrating that there is an interest in open source by IT leaders).

[236] Angela Kallhoff, *Public Goods as Obligatory Bridges Between the Public and the Private*, 50 PHIL. PAPERS 387, 387–88 (2021).

services;[237] publicly provisioned, such as national defense;[238] or provisioned by every member of society, such as environmental preservation.[239] The only two requirements are that they be non-excludable, in that no one can be prevented from using them, and non-rivalrous, in that everyone can use them at once.[240] Open source consists of two components: the software and its maintenance. The former is a pure public good, but the latter is not. Because the two components are inseparable in practice, open source amounts to an impure public good.

1. Characteristics of a Public Good

Public goods must be non-excludable and non-rivalrous.[241] While public goods can inherently possess these qualities, this Article focuses on public goods that are made non-excludable and non-rivalrous by virtue of policy and dedicated effort. In those cases, we *choose* not to exclude people and we do what is needed to keep ahead of demand.

A good is excludable if individuals can be prevented from consuming it.[242] Some public goods, as discussed above, are non-excludable by nature, such as air. Other public goods, such as education, are made non-excludable through policy.[243] The law mandates universal access to public schools;[244] private schools are free to deny applicants.[245]

[237] Lindsay F. Wiley, *Privatized Public Health Insurance and the Goals of Progressive Health Reform*, 54 U.C. DAVIS L. REV. 2149, 2149, 2208–09 (2021) ("Washington's health insurance exchange featured fifteen plans touted as public options, offered by five private carriers. . . . Reliance on private markets to determine the distribution of health care goods and services has allowed American voters to side-step public deliberations on difficult decisions regarding which people and which conditions trigger collective responsibility for health and wellbeing."); Julian Reiss, *Public Goods*, STANFORD ENCYC. PHIL. (July 21, 2021), https://plato.stanford.edu/entries/public-goods/ [https://perma.cc/H4XY-DFPG] ("Individuals benefit from a healthy population in a variety of ways. . . . These benefits obtain in a non-excludable and non-rivalrous manner. A healthier population is also more likely to be productive, making public health analogous to education.").

[238] Reiss, *supra* note 237.

[239] Kirsten H. Engel, *The Dormant Commerce Clause Threat to Market-Based Environmental Regulation: The Case of Electricity Deregulation*, 26 ECOLOGY L.Q. 243, 251 (1999) ("Environmental regulation is necessary from an economic standpoint because it corrects for the market's failure to internalize the costs of pollution or to generate an efficient amount of public goods such as clean air.").

[240] *See* RICHARD A. MUSGRAVE, THE THEORY OF PUBLIC FINANCE: A STUDY IN PUBLIC ECONOMY 13–14 (1959); Paul A. Samuelson, *The Pure Theory of Public Expenditure*, 36 REV. ECON. & STAT. 387, 387 (1954).

[241] *See* Samuelson, *supra* note 240, at 387.

[242] Reiss, *supra* note 237.

[243] *See* Harold Demsetz, *The Exchange and Enforcement of Property Rights*, 7 J.L. & ECON. 11, 18 (1964).

[244] *Your Right to Equality in Education*, ACLU, https://www.aclu.org/other/your-right-equality-education [https://perma.cc/KU47-89Z5].

[245] E.A. Gjelten, *Can Private Schools Discriminate Against Students?*, LAWYERS.COM (Feb. 5, 2019), https://www.lawyers.com/legal-info/research/education-law/can-private-schools-discriminate-against-students.html [https://perma.cc/JT4R-5XU4 (staff-uploaded archive)].

A good is rivalrous if one individual's consumption of it inhibits another person's ability to benefit from it—in other words, rivalrous goods are depletable.[246] A non-rivalrous good, by contrast, must be able to accommodate existing use and scale up with increased demand. A good is perfectly non-rivalrous if it is infinitely available, in that a limitless number of people can use it at once and that it will not run out. Some public goods, like air, are inherently non-rivalrous; although they are technically depletable—a person alone in a vacuum chamber will eventually asphyxiate—their supply is automatically replenished under natural conditions. Replenishing the supply of goods that are not inherently non-rivalrous takes concerted effort and investment.

Realistically, most goods treated as public goods are not perfectly non-rivalrous.[247] Public goods that are, to some degree, rivalrous, are called "common pool resources,"[248] or impure public goods. Though they are not infinitely available,[249] they possess the quality of "basic availability," which requires that each person be able to consume the same amount of and receive the same benefit from the common resource *up to* a certain predetermined, good-specific threshold—such as the capacity for cars on a road.[250]

Preserving the non-rivalry of impure public goods requires ensuring supply meets rising demand (increasing the capacity threshold) and does not deteriorate.[251] Impure public goods can be depleted if they are overused.[252] A heavily used road without routine maintenance will be riddled with potholes and rendered unusable. Similarly, a network of roads supporting an explosively growing community will become rapidly congested. Without the development of new highways to siphon off some of the traffic, the public will suffer gridlock. Therefore, preserving non-rivalry demands routine maintenance, which requires dedicated efforts and resource investments.

[246] Reiss, *supra* note 237.

[247] Inge Kaul, Isabelle Grunberg & Marc A. Stern, *Defining Public Goods*, *in* GLOBAL PUBLIC GOODS: INTERNATIONAL COOPERATION IN THE 21ST CENTURY 2, 3–4 (Inge Kaul, Isabelle Grunberg & Marc A. Stern eds., 1999).

[248] *See generally* Elinor Ostrom, *How Types of Goods and Property Rights Jointly Affect Collective Action*, 15 J. THEORETICAL POL. 239, 239 (2003) (describing "common pool resources").

[249] David W. Barnes, *Congestible Intellectual Property and Impure Public Goods*, 9 NW. J. TECH. & INTELL. PROP. 533, 538 (2011).

[250] ANGELA KALLHOFF, WHY DEMOCRACY NEEDS PUBLIC GOODS 16–18 (2011).

[251] David W. Barnes, *The Incentives/Access Tradeoff*, 9 NW. J. TECH. & INTELL. PROP. 96, 103–04 (2010); CORNES & SANDLER, *supra* note 99, at 8 (positing that a good is non-rivalrous "when a unit of the good can be consumed by one individual without detracting, in the slightest, from the consumption opportunities still available to others from that same unit").

[252] *See* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 442 (2015).

2. Open Source as a Public Good

For all intents and purposes, open source is a public good, albeit an impure one; it is not inherently non-excludable and non-rivalrous, but it endeavors to be both.[253] In this way, it is akin to critical infrastructure security[254] and cybersecurity information,[255] both considered public goods, despite the fact that critical infrastructure resources can be rivalrous and cybersecurity information protected by firms as proprietary can be excludable. The public goods framework remains useful because it casts light on the unique market forces governing open source.

a. Non-Excludable

Open source is non-excludable because the open-source community decided to make it available to everyone for free.[256] Closed-source software excludes users by making the source code confidential and limiting access with licenses. Though open source could do the same,[257] the community instead took pains to make the software non-excludable: they published the source code online, they chose not to impose minimal restrictions on use, they forgo collecting a fee, and they distribute the code via a license that preserves its openness. Open source's express purpose is to be a non-excludable contribution to the digital commons.[258]

b. Somewhat Rivalrous

Open source is made up of two components—the code itself, which is inherently non-rivalrous, and the maintenance required to support it, which is not. Maintenance is required to ensure the code *remains* non-rivalrous. When the demand for maintenance exceeds the supply, then the community is being

[253] *See* Benkler, *supra* note 193, at 377, 404.

[254] *See* CORNES & SANDLER, *supra* note 99, at 4–5; *cf.* TODD SANDLER & KEITH HARTLEY, THE ECONOMICS OF DEFENSE 58 (1995).

[255] *See generally* ROSENZWEIG, CYBERSECURITY AND PUBLIC GOODS, *supra* note 159 (discussing cyberspace and the role the government and private actors play).

[256] *See* Jyh-An Lee, *New Perspectives on Public Goods Production: Policy Implications of Open Source Software*, 9 VAND. J. ENT. & TECH. L. 45, 76 (2006) [hereinafter Lee, *Public Goods Production*] (describing the "public goods nature" of OSS); Schmidt & Schnitzer, *supra* note 36, at 473–74 (posing the following question: "Why do programmers voluntarily contribute to the public good of open source, even if there are no direct financial rewards?"); BLIND ET AL., *supra* note 28, at 35–36 (discussing scholarship that characterizes open source as a public good).

[257] *See* John P. Conley & Christopher S. Yoo, *Nonrivalry and Price Discrimination in Copyright Economics*, 157 U. PA. L. REV. 1801, 1806 (2009) (noting that goods that are technically excludable but perhaps costly or otherwise difficult to exclude could be considered a public good).

[258] Allen K. Yu, *Enhancing Legal Aid Access Through an Open Source Commons Model*, 20 HARV. J.L. & TECH. 373, 378 (2007) ("Open source is one of the most successful commons movements ever created.").

overused, which can cause software quality and security to deteriorate.[259] Poorly maintained code is insecure because vulnerabilities are left unresolved; if left insecure, one user's vulnerable project can threaten every other user of the project, interfering with their use of the code.

Open-source software, like all software, is inherently non-rivalrous, because an infinite number of copies can be made without impacting any given user. In this way, it is like literature; Moby Dick can be reprinted an infinite number of times without ever impacting the value of the text.

But in other, important ways, open source is rivalrous. Open-source maintenance, a necessary component of open source, is dependent on a finite community with limited capacity to support its projects.[260] While Moby Dick is theoretically infinitely reproducible, reprinting it requires a publishing house, employees, printing presses, and ink—support structures that have limited capacity. Similarly, open-source projects are only as non-rivalrous as they are maintained. Just as printing more copies of a book requires more supplies, an increased demand for open-source projects requires more maintenance. As projects grow in popularity or size, maintenance takes more time, because there are more reports, pull requests, and lines of code to review.[261]

Currently, the burden of maintenance tends to fall on the open-source community alone. Instead, it should be shared by two parties: the open-source community and its primary beneficiaries. The open-source community contributes to the code, scans the code for vulnerabilities, patches vulnerabilities, reviews pull requests, resolves conflicts, and keeps an eye out for public vulnerability disclosures. Think of this party as the maintenance workers hired by the government to repave a road with potholes.

Open-source security also relies on its consumers, who should also be checking for vulnerabilities and implementing patches. Think of them as the drivers who regularly use a road. It is on them to ensure that a bridge's weight limit is not exceeded, that their car is not leaking oil that could cause a pile-up, and that dangerous potholes are reported. Without their responsible use, a road would deteriorate rapidly to the detriment of all other users. In addition to taking due care in using open source, consumers must also contribute to its

[259] *See, e.g.*, JimBobSquarePants (@James_M_South), TWITTER (July 12, 2020, 3:29 PM), https://twitter.com/James_M_South/status/1282396639714373632 [https://perma.cc/7ZSC-9LTL] (describing how the growth of a library the author maintains concerns him because of the lack of developer support he has, including by corporate users of his library).

[260] As discussed in Section I.B, the open-source community consists of volunteers.

[261] Valsorda, *supra* note 129 ("The workload increases as the project grows, but the team struggles to get more resources, no one gets promoted, and people burn out and leave or change roles. I've seen this play out across multiple companies and ecosystems, over and over.").

supply just as highway users pay taxes to fund road maintenance.[262] Contributing Consumers are already doing this, but they are the minority.

In this way, open source's non-rivalry depends as much on the behavior of its consumers as it does on the dedication of its community.[263] When roads increase in popularity, the importance of any one driver behaving responsibly increases, because the fallout of an accident would be more severe. Similarly, as open source's popularity continues to skyrocket, so does the threat posed by Irresponsible Consumers.

B. *Open Source's Market Failures*

Because open source is an impure public good, market failures can result in its overuse and eventual depletion. Market failures, or inefficiencies in the provisioning of a good, are outgrowths of an imperfect free-market system.[264] They are endemic to public goods—open source is no exception. Open source's market failures manifest as a free-rider problem, negative externalities, and asymmetric information.[265] At the source of each is the Irresponsible Consumer.

1. Free Riders

The root cause of the open-source security problem is the free-rider problem. The cost of supplying open source includes the cost of maintaining and securing open source, which requires investments by the open-source community and its consumers. Because open source is non-excludable, companies can profit from it without paying a dime—and many do.[266] This results in a lack of investment in the maintenance required to prevent overuse.

[262] JOSEPH E. STIGLITZ, WHITHER SOCIALISM? 7 (1994) [hereinafter STIGLITZ, WHITHER SOCIALISM?] ("Markets cannot provide public goods, and hence the rationale for public expenditures on roads, defense, and other public works.").

[263] Pattison-Gordon, *supra* note 77 ("Creating secure code is only part of the fix—users adopting that software also need to maintain it well. That includes ensuring they implemented the code in ways that don't introduce vulnerabilities.").

[264] *See* NICK HANLEY, JASON F. SHOGREN & BEN WHITE, ENVIRONMENTAL ECONOMICS IN THEORY AND PRACTICE 24 (1997).

[265] *See* Joseph E. Stiglitz, *The Theory of Local Public Goods Twenty-Five Years After Tiebout: A Perspective* 24, 29, 35 (Nat'l Bureau of Econ. Rsch., Working Paper No. 954, 1982) (discussing the free-rider problem and externalities); Patrick W. Schmitz, *Optimal Ownership of Public Goods Under Asymmetric Information*, 198 J. PUB. ECON. 1, 4 (2021) (discussing the issue of asymmetric information in the context of public goods).

[266] Jonathan Anomaly, *Public Goods and Government Action*, 14 POL. PHIL. & ECON. 109, 120 (2015) (explaining that "as the number of people needed to produce a public good increases, strategic behavior is likely to emerge," such as free riding).

Scholars have explored how corporate cybersecurity has characteristics of a public good and suffers the free-rider problem.[267] They explain how the non-excludability of cybersecurity results in underinvestment and the prevalence of poor security practices.[268] Corporate software itself, however, is not a public good and therefore functions closer to a free-market system than open-source software. In a competitive market, the price reflects the net value of the good to society, which, in theory, results in the efficient production of a good. Corporate producers of cybersecurity can adjust price to reflect demand, ensuring that they are sufficiently incentivized and compensated for ratcheting up production.[269] Indeed, we are seeing technology companies invest in privacy-by-design, creating more secure products in response to heightened consumer demand for privacy-protecting measures. Consumer incentives to pay the price are tied to the excludability of a good—the risk of deprivation spurs positive action.

Open source is designed to be free and non-excludable, which means it lacks the incentives that drive responsible consumption.[270] Without these market pressures, consumers maximize self-interest—they use without paying, leading to overuse.[271] Therefore, "[i]nstead of contributing to the sustenance and provision of public goods, the most likely behavior is free-riding on the efforts of others who together sustain the public good."[272] This shortchanges the

[267] *See generally* Tabrez Y. Ebrahmi, *National Cybersecurity Innovation*, 123 W. VA. L. REV. 483 (2020) (discussing both cybersecurity and the free-rider problem that exists within the cyber realm while exploring whether the government or markets will develop innovative solutions to these issues).

[268] *See* Lawrence A. Gordon & Martin P. Loeb, *The Economics of Information Security Investment*, 5 ACM TRANSACTIONS ON INFO. & SYSTEM SEC. 438, 438–39 (2002) (describing inadequate investments in corporate cybersecurity to reduce data breaches and develop encryption, access control, and firewalls to protect information); *see also* Joe Mariani, Tim Li, Chris Weggeman & Pankaj Kamleshkumar-Kishnashi, *Incentives Are Key To Breaking the Cycle of Cyberattacks on Critical Infrastructure*, DELOITTE (Mar. 8, 2022), https://www2.deloitte.com/us/en/insights/industry/public-sector/cyberattack-critical-infrastructure-cybersecurity.html [https://perma.cc/F7UC-SUXZ] ("If cybersecurity of critical infrastructure is a known and important problem and yet progress toward greater security has been slow, it implies that there are other pressures on peoples' decision-making. In other words, there are incentives tugging many stakeholders—including owners of critical infrastructure—away from actions that support security.").

[269] Bruce Schneier, *Security Economics of the Internet of Things*, SCHNEIER ON SEC. (Oct. 10, 2016), https://www.schneier.com/blog/archives/2016/10/security_econom_1.html [https://perma.cc/7NCR-TKAA] (describing the market incentives that explain why "Microsoft, Apple, and Google spend a lot of time testing their code before it's released, and quickly patch vulnerabilities when they're discovered").

[270] *See* Lee, *Public Goods Production*, *supra* note 256, at 50–51 ("Unlike property in proprietary software, 'property in [OSS] is configured fundamentally around the right to distribute, not the right to exclude.'" (quoting STEVEN WEBER, THE SUCCESS OF OPEN SOURCE 1 (2004))).

[271] Sarwat Jahan & Ahmed Saber Mahmud, *What Is Capitalism?*, INT'L MONETARY FUND, June 2015, at 44, 44, https://www.imf.org/external/pubs/ft/fandd/2015/06/pdf/basics.pdf [https://perma.cc/C5V7-9HD4].

[272] Kallhoff, *supra* note 236, at 391.

open-source community, those charged with the "sustenance and provision" of open-source software, by denying them necessary resources and the benefit of responsible open-source consumers. Free-riding is an exploitation of the producers of open-source maintenance and security, and results in a deficient supply.[273]

The most egregious examples of free-riders in open source are the Irresponsible Consumers. These entities could be contributing to projects in a variety of meaningful ways: as funders, coders, or organizers.[274] As discussed earlier, many of them use un- or undermaintained open-source projects that could use each type of contribution. Despite the obvious need for support, Irresponsible Consumers do not donate funds to the community or contribute paid-developer time to the project's upkeep.[275] International security standards specifically calls on open-source consumers to "always share" their risk information and patches "with the upstream [users and maintainers] to ensure that security fixes are integrated in upcoming versions" to "fulfill the need for long-term maintenance."[276] Even still, Irresponsible Consumers choose to free ride on open-source maintenance.

Many Irresponsible Consumers also free ride on investments that Contributing Consumers, which includes their competitors, make in the open-source community. Google, one such Contributing Consumer, acknowledges that "[t]he more open source developers there are in the world, the healthier and more sustainable the entire community will be."[277] Accordingly, ten percent

[273] Felten & Kroll, *supra* note 125 (stating that OpenSSL, an open-source security protocol, "is a public good with the attendant funding problems: once it exists, no one can be prevented from benefiting from it, so many hope for a free ride on someone else's dime").

[274] *See* Shah & Nagle, *Why Do User Communities Matter for Strategy?*, *supra* note 67, at 21, 31.

[275] Danny Grander & Liran Tal, *A Post-Mortem of the Malicious Event-Stream Backdoor*, SNYK (Dec. 6, 2018), https://snyk.io/blog/a-post-mortem-of-the-malicious-event-stream-backdoor/ [https://perma.cc/7WQY-C9HJ] ("If widely used packages, such as event-stream, were supported by just a small proportion of those who consume it, and take value from it, the malicious takeover could easily have been avoided.").

[276] *Manage Vulnerabilities in ICS Open Source Software*, *supra* note 54 ("To maximize the power of OSS, it's important not to use open source as a closed source. This way, you can avoid wasting resources on the inevitable need to fix code conflicts after merging every new version of the latest OSS release. All users will benefit from the rule of 'upstream first,' including the contributors themselves.").

[277] *Frequently Asked Questions*, GOOGLE SUMMER CODE, https://developers.google.com/open-source/gsoc/faq [https://perma.cc/34X7-RLB6]. In the past year, some companies have also decided to launch funds that support open source. *See, e.g.*, Paul Sawers, *Appwrite Launches Fund To Help Sustain Open-Source Software Development*, VENTUREBEAT (May 4, 2022, 6:00 AM), https://venturebeat.com/dev/appwrite-launches-fund-to-help-sustain-open-source-software-development/ [https://perma.cc/3J5M-7JPU]; Aisha Malik, *Spotify Launches New Fund To Support Independent Open Source Projects*, TECHCRUNCH (Apr. 25, 2022, 10:40 AM), https://techcrunch.com/2022/04/25/spotify-fund-support-independent-open-source-projects/ [https://perma.cc/X8NX-ST6W].

of its developers actively contribute to open-source projects.[278] Irresponsible Consumers free ride on this corporate altruism, benefitting from the marginal increase in available support.[279] Ironically, by free riding, Irresponsible Consumers forego substantially higher returns—research has found that paying employees to contribute upstream can boost productive use of that open-source software by as much as 100%.[280]

Not all free-riders are driven by the same motivations. Some Irresponsible Consumers would contribute to open source, but only if their contributions were sure to benefit them.[281] Their contributions are conditioned on the initial investment of other parties. This implies the existence of a tipping point—a point at which others are contributing enough that any dollar a new contributor spends yields positive returns. To overcome these free-riding problems, some consumers need to take on the risk and burden of acting as the first movers. Closed-source code does not face the same problem—generally, all customers pay the same price to access the good.

Other Irresponsible Consumers, however, are unconditional free-riders, who will never invest in open source because they assume the rest of the ecosystem will take on the cost of securing open source.[282] With closed-source code, only the supplier can secure its software; with open-source code, anyone can secure it and large open-source consumers who stand to lose a lot will take the appropriate steps. Accordingly, they scan for vulnerabilities, responsibly disclose vulnerabilities identified, implement patches made available, contribute to the development of patches, replace outdated components with updated versions, and shift away from relying on unsupported projects. In taking these measures, these Contributing Consumers bolster their own security, thereby bolstering the security of the whole ecosystem—rising tides lift all ships. Therefore, an Irresponsible Consumer using the same project as a

[278] Sophia Vargas, *Metrics, Spikes, and Uncertainty: Open Source Contribution During a Global Pandemic*, GOOGLE OPEN SOURCE BLOG (Aug. 18, 2021), https://opensource.googleblog.com/2021/08/metrics-spikes-and-uncertainty-open-source-contribution-during-a-global-pandemic.html [https://perma.cc/74QH-W3BM]; *see also* Sawers, *supra* note 277; Malik, *supra* note 277.

[279] Matt Asay, *Enterprises Want More Open Source Yet Won't Pay Developers To Work on It*, TECHREPUBLIC (Nov. 2, 2018, 1:44 PM), https://www.techrepublic.com/article/enterprises-want-more-open-source-yet-wont-pay-developers-to-work-on-it/ [https://perma.cc/9D9Y-MNDV]; EGHBAL, *supra* note 116, at 106.

[280] Kristen Senz, *The Hidden Benefit of Giving Back to Open Source Software*, HARV. BUS. SCH. (Sept. 5, 2018), https://hbswk.hbs.edu/item/the-hidden-benefit-of-giving-back-to-open-source-software [https://perma.cc/LV2V-LB25].

[281] Marie-Claire Villeval, *Contribution to Public Goods and Social Preferences: Recent Contributions from Behavioural Economics*, 63 ECON. REV. 389, 389–420 (2012).

[282] Sean Collins, *Relay the Right Way: Harnessing Heterogeneity in Sequential Team Production*, 37 MANAGERIAL & DECISION ECON. 407, 418 (2016).

Contributing Consumer like Google can, understandably, expect Google to take on the burden of supporting that project's maintenance—it has more to lose. The general assumption is that a popular open-source library is sure to be secure, given how many eyes are on it.[283]

By free-riding, Irresponsible Consumers are overusing the existing supply of open-source maintenance. Without an injection of resources and the adoption of responsible security practices, open-source maintenance cannot meet demand, leaving open source and the critical infrastructure it supports vulnerable.

2. Cost of Externalities Fall on Public

The free-rider problem results in the overuse of open-source maintenance, which in turn leads to the proliferation and persistence of vulnerabilities in our critical infrastructure. Externalities are under- or overvalued aspects of a public good that occur when private costs or benefits and social costs or benefits diverge.[284] As the discrepancy increases, private decisions are less and less likely to lead to efficient resource use.[285] With open source, the risk of a vulnerability threatens the public more than the private company.[286] Because of this, private companies are not making security decisions with the public's wellbeing in mind. Ultimately, the public suffers the cost of the private sector's decision to free ride.

Externalities are not a problem when private decisions have ancillary public benefits. With positive externalities, private actors maximizing self-interest can have unintended, positive impacts on society.[287] For example, the advent of social media platforms were profitable for the companies, but the technology also enabled grassroots resistance to authoritarian regimes.[288]

[283] Jeff Williams, *Removing a False Sense of (Open Source) Security*, 2020 COMP. FRAUD & SEC. 8, 9–10.

[284] ROBERT COOTER & THOMAS ULEN, LAW & ECONOMICS 44–47 (4th ed. 2004); *see* Michael J. Trebilcock & Edward M. Iacobucci, *Privatization and Accountability*, 116 HARV. L. REV. 1422, 1431–35 (2003). *See generally* ARTHUR CECIL PIGOU, THE ECONOMICS OF WELFARE (3d ed. 1920) (developing the economic externality concept).

[285] Mollie Lee, Note, *Environmental Economics: A Market Failure Approach to the Commerce Clause*, 116 YALE L.J. 456, 480 (2006) [hereinafter Lee, *Environmental Economics*].

[286] For example, see the wide-spread, network issues related to the open-source project Express Gateway. Jack Gillum & William Turton, *The White House Is Worried About Open Source Software Security*, BLOOMBERG (Jan. 19, 2022), https://www.bloomberg.com/news/articles/2022-01-19/log4j-vulnerability-shows-risk-of-relying-on-open-source-volunteer-coders [https://perma.cc/E367-BSPU].

[287] *See* JOSEPH E. STIGLITZ, ECONOMICS OF THE PUBLIC SECTOR 219, 223 (2d ed. 1988).

[288] *See* Heather Brown, Emily Guskin & Amy Mitchell, *The Role of Social Media in the Arab Uprisings*, PEW RSCH. CTR. (Nov. 28, 2012), https://www.pewresearch.org/journalism/2012/11/28/role-social-media-arab-uprisings/ [https://perma.cc/4MV7-7WKJ].

Indeed, society benefits from the fact that open source has cascading, network effects.[289]

Externalities are harmful when private decisions harm the public more than the transacting parties. As an enabling technology, open source is "a means to other ends," and so its "effectiveness, efficiency, and reliability of its contribution to these other ends must ultimately be the measure of infrastructure performance."[290] To the public, reliability is more than software functionality—it is also software's resilience against attack.[291] Scholars recognize that the cumulative effect of open-source security and reliability affects the public uniquely, but that the externality is not internalized by the companies.[292]

This is because incongruous incentives: overuse resulting in an exploited vulnerability can be expensive for a company, but downed critical infrastructure would be life-threatening to society.[293] When the Log4Shell vulnerability was exploited, companies and governments bore the cost of shutting down systems suspected of containing the vulnerability and investing the resources to patch it, not to mention the impact on the trust and reputation of the company.[294] Users bore the cost of system failures and the possibility that their sensitive information was compromised.[295] Belgium's Defense Ministry said it shut down parts of its computer network because attackers triggered the vulnerability, directly impacting the government's ability to protect national security.[296] Quebec shut down parts of its computer network, including thousands of sites related to the provision of higher education, directly impacting the government's ability to continue public service delivery.[297]

[289] *See* Frischmann, *supra* note 80, at 932.

[290] NAT'L RSCH. COUNCIL, MEASURING AND IMPROVING INFRASTRUCTURE PERFORMANCE 5 (1996).

[291] *See* Frischmann, *supra* note 80, at 958–59.

[292] *See generally* Micah Schwalb, *Exploit Derivatives & National Security*, 9 YALE J.L. & TECH. 162 (2007) (describing national defense software insecurity as a negative externality that impacts the public but is not internalized by the transaction).

[293] Chris Teale, *Water Utility Cyber Investments Stymied by Unfunded Mandates, Fiscal Pressures*, GCN (Sept. 26, 2022), https://gcn.com/cybersecurity/2022/09/water-utility-cyber-investments-stymied-unfunded-mandates-fiscal-pressres/377639/ [https://perma.cc/X36V-V3X6] (quoting Representative John Katko (R-N.Y.) as saying that "the incident in Oldsmar in which hackers altered the chemicals in the water treatment system and could have endangered residents had they not been stopped 'demonstrated first-hand the devastating, real-world consequences that a cyber attack can have'").

[294] *See* Uberti et al., *supra* note 2 ("[A] flaw in widely used internet software known as Log4j has left *companies and government officials* scrambling to respond . . . ." (emphasis added)).

[295] *See, e.g.*, *Log4j Vulnerability—What Everyone Needs To Know*, NAT'L CYBER SEC. CTR., https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know [https://perma.cc/FX8D-FB9N] (describing how the vulnerability could let attackers steal passwords, logins, and extract personal data).

[296] Uberti et al., *supra* note 2.

[297] Paganini, *supra* note 6.

Because the public depends more on open-source security than the company, the Irresponsible Consumer underinvests in its preservation. Software bugs are inevitable, so monitoring should be factored in as a cost of using software.[298] But "fixing bugs and protecting systems yields little direct return on investment, impedes time to market, and oftentimes undermines system usability; thus, manufacturers understandably sacrifice cost-incurring security for value-added functionality."[299] While this is true for all code, it is especially true for open-source code, where Irresponsible Consumers are rarely held accountable for the fallout of an exploit.[300] Irresponsible Consumers generally conclude that it is not worth investing in preventive measures, no matter how severe the threatened damage.[301]

In the absence of externalities, the free exchange of private goods leads to investments that benefit some and leave no one worse off.[302] If companies bore the entire cost of insecure networks, they would be incentivized to bolster security measures rather than suffer the higher cost of the preventable damage. If there were market players who were unable to invest in these security measures, then the market would compensate for them; insecurity becomes intolerable when the market is forced to bear the cost.[303] However, "[s]ince individuals in a market system respond only to the benefits and costs that they actually receive and pay for, the market system may be inadequate to deal with externalities."[304]

Open source's inability to shift the cost of insecure critical infrastructure onto the parties introducing the risk is evidence of a market failure.[305] These externalities are caused and exacerbated by the free-rider problem; because

[298] Robert N. Charette, *Why Software Fails*, IEEE SPECTRUM ONLINE (Sept. 1, 2005), https://spectrum.ieee.org/why-software-fails [https://perma.cc/Q22L-4VSB].

[299] Schwalb, *supra* note 292, at 169.

[300] L. Jean Camp & Catherine D. Wolfram, *Pricing Security*, *in* ECONOMICS OF INFORMATION SECURITY 17, 21–22 (L. Jean Camp & Stephen Lewis eds., 2004) (noting market failures in cybersecurity); Ebrahmi, *supra* note 267, at 521–26 (same).

[301] *See* Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333, 1342–43 (2006) (discussing how companies are not incentivized to invest in additional security measures if (1) the organization does not know there is a security issue and/or (2) the market or other mechanisms are not effective for disciplining the party).

[302] *See generally* ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS (Hartford: Lincoln & Gleason, 4th ed. 1804) (1776) (providing a landmark economic discussion of the division of labor, productivity, and free markets).

[303] *See id.* at 295–96 (describing how markets compensate for members unable to contribute by promoting specialization and the division of labor and creating derivative markets to meet demand).

[304] Darren Bush, *The "Marketplace of Ideas:" Is Judge Posner Chasing Don Quixote's Windmills?*, 32 ARIZ. STATE L.J. 1107, 1109 n.17 (2000) (noting that all of human behavior can be understood as exchange relationships).

[305] *See* ELIZABETH ANDERSON, VALUE IN ETHICS AND ECONOMICS 143–59 (1993).

companies cannot prevent others from free riding on their security investments, they themselves are incentivized to free ride.[306]

3. Asymmetric Information

Asymmetric information, or an information imbalance, is another market failure, one that impedes efforts to rectify the free-rider and externality problems.[307] Economic theory dictates that perfect information is a necessary precursor to avoiding overuse and allocating resources efficiently to provide the optimal supply of a good.[308] While all markets suffer from imperfect information, public goods markets lack the incentives built into competitive markets that promote information sharing.[309] Without access to accurate, complete information about the open-source ecosystem, efforts to secure open source will fall short.[310]

This opacity means that parties are unable to allocate resources efficiently. A threshold barrier is that it is hard to establish the true value of an open-source project. This, in turn, makes it difficult for companies to efficiently internalize negative externalities. Internalizing negative externalities requires shifting public costs onto the transacting parties.[311] In the private sector, the market can accomplish this through price calculation.[312] In establishing a price, parties

[306] Schmidt & Schnitzer, *supra* note 36, at 483–84 ("Because companies cannot prevent others from benefiting from its investment in open-source, companies have a strong incentive to free ride on the contributions of others to open source, and their subsidies to OSS development are likely to remain limited.").

[307] NICK HANLEY, JASON F. SHOGREN & BEN WHITE, ENVIRONMENTAL ECONOMICS IN THEORY AND PRACTICE 68–75 (2d ed. 2007).

[308] *See* Yafit Lev-Aretz & Katherine J. Strandburg, *Regulation and Innovation: Approaching Market Failure from Both Sides*, 38 YALE J. ON REGUL. BULL. 1, 9–12 (2020).

[309] *See* Schmitz, *supra* note 265, at 4–5 (discussing the issue of asymmetric information in the context of public goods).

[310] Avi Press, *How Open-Source Distribution Data Can Help To Make the Software Supply Chain More Secure*, FORBES (Aug. 15, 2022, 6:30 AM), https://www.forbes.com/sites/forbestechcouncil/2022/08/15/how-open-source-distribution-data-can-help-to-make-the-software-supply-chain-more-secure/?sh=17c4f1fd109a [https://perma.cc/C2R9-SKP7] ("The core of a potential solution is better data. If maintainers knew which organizations relied on their software, they'd be in a much better position to help those people upgrade and patch the vulnerability. They could identify where to deploy effort and resources in fixing the problem proactively at scale. In fact, the data could even unlock a new industry—for companies to offer consultation and support services related to these key open-source vulnerabilities. However, none of this works without knowing who you need to help.").

[311] *See* GEORGE J. STIGLER, THE THEORY OF PRICE 113 (3d ed. 1966). *See generally* R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960) (describing the role of transaction costs in economic systems and institutions).

[312] *See* Daniel F. Spulber & Christopher S. Yoo, *Access to Networks: Economic and Constitutional Connections*, 88 CORNELL L. REV. 885, 919, 921, 926 (2003) (assuming that if competitive markets can form, then "market prices [will] continue to be an accurate measure of value").

maximize self-interest and are incentivized to share information to do so.[313] But there is no obvious way of measuring collective demand for a public good.[314] Without a competitive market, valuing open source requires voluntary coordination and information sharing.[315] The private sector is not incentivized to do either. In fact, without competitive market pressures, consumers are incentivized to conceal their preferences.[316]

To allocate resources to the projects most in need, the market must know which projects critical infrastructure relies on and which projects have the biggest resource deficits and present the greatest risk.[317] With closed-source code, a diligent company has insight into all its vendors, from which it obtains software, and customers, to whom it sells software. A well-maintained paper trail can uncover the popularity and uses of any given product. As discussed earlier, neither maintainers nor project-users know every location where a project is being used and what it is being used for, and companies are not incentivized to maintain documentation of their open-source usage. Even a diligent open-source consumer that wants to identify all their open-source dependencies may not be technologically able to.

While some degree of information can be obtained by project downloads and insight into the projects used by important market players, such as Google, there will always be projects that may have modest consumer bases but are used

[313] *See* F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 525–28 (1945).

[314] Samuelson, *supra* note 240, at 388 (discussing the inability of a competitive market to find the optimal amount of a public good that must be provided or consumed); Patricia A. Champ, *Collecting Survey Data for Nonmarket Valuation*, *in* A PRIMER ON NONMARKET VALUATION 59, 59 (Patricia A. Champ, Kevin J. Boyle & Thomas C. Brown eds., 2003) ("The unique nature of environmental and natural resource amenities makes valuation a challenge in many respects. Prices reflect aggregate societal values for market goods, but nonmarket goods lack an analogous indicator of value.").

[315] Benkler, *supra* note 193, at 375 ("Where agents, efforts, or resources cannot be so specified, they cannot be accurately priced or managed. The process of specification creates two sources of inefficiency. First, it causes information loss. Perfect specification is unattainable because of transaction costs associated with specifying the characteristics of each human and material resource and each opportunity for utilization.").

[316] HANLEY ET AL., *supra* note 307, at 61–74.

[317] David Forscey, Jon Bateman, Nick Beecroft & Beau Woods, *Systemic Cyber Risk: A Primer*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Mar. 7, 2022), https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531 [https://perma.cc/VGB6-YAMR] ("The difficulty of mapping and measuring systemic cyber risk presents at least two policy problems. First, without the ability to understand and communicate the probability and severity of systemic cyber events, decisionmakers cannot determine whether resources currently devoted to other problems (including other forms of cyber risk) should be redirected toward steps to mitigate systemic cyber risk. Second, without a clear picture of where the problem areas lie and which possible failure points deserve the most attention, policymakers cannot determine precisely which resources should be redirected and how.").

by entities providing National Critical Function.[318] The local wastewater management system almost certainly uses some amount of open-source software but, given the tendency for less-sophisticated, resource-strapped consumers to rely on legacy systems rather than updating their technology, the open-source library they rely on might have been abandoned.[319] The threat against these smaller utilities is hardly speculative—there have been seven separate ransomware attacks on government-owned water facilities that have become public since 2019.[320] Without a comprehensive inventory of open-source components, it is impossible to identify overused or unsupported projects and allocate resources to support these small critical infrastructure entities.

Asymmetric information prevents the market from addressing the exposed weaknesses in the ecosystem. It is impossible to scan for vulnerabilities or available patches for open-source projects without knowing which projects the products use. It is impossible for a maintainer to identify all downstream users of a software vulnerability if they do not know who their customers are or

[318] For example, in 2019, researchers revealed previously undisclosed security vulnerabilities inside an operating system called VxWorks that was not especially popular but was used primarily in settings like aviation and industrial automation where physical safety is essential. Scott Ferguson, *'Urgent/11' Vulnerabilities Affect Many Embedded Systems*, BANK INFO SEC. (July 30, 2019), https://www.bankinfosecurity.com/urgent11-vulnerabilities-affect-many-embedded-systems-a-12851 [https://perma.cc/9X45-ATGM]. This single dependency, obscured in the supply chain, imparts remotely triggerable failure modes to over 200 million devices across all critical infrastructure sectors. Jai Vijayan, *Millions More Embedded Devices Contain Vulnerable IPnet Software*, DARKREADING (Oct. 2, 2019), https://www.darkreading.com/vulnerabilities-threats/millions-more-embedded-devices-contain-vulnerable-ipnet-software [https://perma.cc/EE7E-9N3E]; Lily Hay Newman, *An Operating System Bug Exposes 200 Million Critical Devices*, WIRED (July 29, 2019, 11:04 AM), https://www.wired.com/story/vxworks-vulnerabilities-urgent11/ [https://perma.cc/A4PU-GPMB]; *see Urgent/11*, ARMIS (Dec. 15, 2020), https://www.armis.com/urgent11/ [https://perma.cc/74EL-7B63].

[319] Mark Montgomery & Samantha F. Ravich, Opinion, *The Cybersecurity Risk to Our Water Supply Is Real. We Need To Prepare*, WASH. POST (Jan. 3, 2022, 1:36 PM), https://www.washingtonpost.com/opinions/2022/01/03/cybersecurity-risk-water-supply/ [https://perma.cc/F9DQ-ZRKX (dark archive)] ("The United States has approximately 52,000 drinking water and 16,000 wastewater systems, many of which service small communities of fewer than 10,000 residents. These systems operate with limited budgets and even more limited cybersecurity personnel and expertise. The automation of technology that these water utilities implemented over the past two decades to both save money and increase efficiency has also exposed them to malicious cyber activity that could disrupt or manipulate services."); Teale, *supra* note 293 ("Rep. James Langevin (D-R.I.) noted that in a 2021 survey by the Water Sector Coordinating Council, 73% of those surveyed said they had between zero and two employees dedicated to network security, adding that lawmakers 'appreciate the challenges' associated with finances.").

[320] Tim Starks, *U.K. Attack Spotlights Water Sector Vulnerabilities*, WASH. POST (Aug. 23, 2022, 7:47 AM), https://www.washingtonpost.com/politics/2022/08/23/uk-attack-spotlights-water-sector-vulnerabilities/ [https://perma.cc/UC4U-HE9F (dark archive)] [hereinafter Starks, *U.K. Attack*] ("An estimated 70,000 utilities control the water supply in the United States, some very small and thus lacking cyber expertise and the dollars to implement improved defenses."). It is likely that many more incidents have gone unreported.

whether a customer has a product affected by the vulnerability.[321] It is impossible for an open-source developer to design an optimal patch if they do not know why some companies decided not to implement previous patches.[322] It is impossible for a customer to use their market power to demand secure open-source practices if they do not know they are using open source. It is impossible for the government to identify Irresponsible Consumers that fail to implement patches until an exploit happens. And it is impossible to shift the cost of externalities to companies without knowing which ones are free-riding.

The market for closed-source code benefits from transparency; access to information enables market-players to address security problems.[323] Without the same incentives driving information sharing, a public goods market like open source is hampered in its ability to find and fix problems. The nature of a public goods market both creates information gaps and encourages market players to exploit them rather than bridge them.

C. *Consequences of Open Source's Market Failures*

The aggregate effect of open source's market failures creates a tragedy of the commons that is unlikely to resolve itself. But public goods theory suggests a solution to the problem: shifting costs to the least-cost avoider.

1. Tragedy of the Commons

The "tragedy of the commons" is an externality problem in which private actors maximizing self-interest results in the excess use of a freely available resource.[324] Because open-source maintenance is rivalrous, overuse will result in depletion of developer support for projects.[325] When developer support is

[321] Press, *supra* note 310 ("Remember that open-source code is repackaged and redistributed in complex ways. It's not just about your primary users; it's also about *their* users, their users' users and so on. Things get more and more complex as you move through the layers of abstraction. For maintainers, there is very little they can do currently to track how their code is being used.").

[322] Sometimes, a company will make the risk calculus not to patch a vulnerability if the patch they are offered is not compatible with their software configuration. Maintainers want access to this information to understand how to build patches that best serve most of their users.

[323] Admittedly, many members of the commercial software industry fail to take advantage of this available benefit. Some fail to document their software components and their transactions. Others, despite having their customer data available, fail to use it to address security problems, either by patching software internally or communicating vulnerability information to their customers.

[324] Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243, 1243–44 (1968).

[325] Charles M. Schweik & Robert English, *Tragedy of the FOSS Commons? Investigating the Institutional Designs of Free/Libre and Open Source Software Projects*, FIRST MONDAY (2007), https://firstmonday.org/ojs/index.php/fm/article/view/1619/1534 [https://perma.cc/LUA7-ZA72] ("Free-riders in this context are programmers, testers or documenters who utilize a particular FOSS software but do not contribute back in these capacities. In a FOSS setting, the tragedy of the commons

overused, developers will be unable to effectively secure the open-source projects society relies on, rendering them vulnerable to attack. If free-riding on the open-source community continues, then the public will suffer the implications of a tragedy of the commons.[326]

Although securing this public good is in every company's self-interest, very few companies want to be the ones to take on that burden. Since everyone has access to open-source code, no single entity feels any obligation to take care of it. Psychologists call this the bystander effect—when multiple parties have the capacity to solve a problem, each individual party feels less responsibility to take action.[327] This results in an elaborate game of chicken—multiple noncoordinating parties holding out for someone else to take on the added cost. The result is a collective action problem that leaves everyone worse off.[328]

In this kind of a tragedy of the commons, private actors acting in their own perceived self-interest are not making efficient decisions. This is emblematic of the prisoner's dilemma, in which two parties—who are not coordinating regarding a decision that affects them both—fail to act in a way that maximizes their overall self-interest.[329] Their best option also presents the greatest risk; it requires both parties to cooperate. If one does not, the other suffers. In open source, because market players do not trust each other to share the cost of securing open source, no one invests in it, hurting everyone.

As is characteristic of a tragedy of the commons problem, this coordination failure will inevitably result in the depletion of a valuable resource, exposing all of society, including the Irresponsible Consumers at fault, to the risk of an exploitation.[330]

comes when there are insufficient human resources available to continue to further develop and maintain the software and, as a result, the software project is abandoned. The project fails to achieve the functionality and use that was perhaps envisioned when it began.").

[326] *See* Hardin, *supra* note 324, at 1246 (referring to the "free-rider problem" as "the tragedy of the commons").

[327] *See* John M. Darley & Bibb Latané, *Bystander Intervention in Emergencies: Diffusion of Responsibility*, 8 J. PERSONALITY & SOC. PSYCH. 377, 377 (1968); Peter Fischer, Joachim I. Krueger, Tobias Greitemeyer, Claudia Vogrincic, Andreas Kastenmüller, Dieter Frey, Moritz Heene, Magdalena Wicher & Martina Kainbacher, *The Bystander-Effect: A Meta-Analytic Review on Bystander Intervention in Dangerous and Non-Dangerous Emergencies*, 137 PSYCH. BULL. 517, 517 (2011).

[328] Schweik & English, *supra* note 325.

[329] A.W. Tucker, *The Mathematics of Tucker: A Sampler*, 14 TWO-YEAR COLL. MATHEMATICS J. 282, 228–30 (1983); *Prisoner's Dilemma*, STANFORD ENCYC. PHIL. (last updated Apr. 2, 2019), https://plato.stanford.edu/entries/prisoner-dilemma/ [https://perma.cc/TGD4-99DS].

[330] *See* Hardin, *supra* note 324, at 1246 (referring to the "free-rider problem" as "the tragedy of the commons").

2. Unaccountable Least-Cost Avoider

Solving the tragedy of the commons problem requires coordinated investment in open-source security. Economic theory tells us that the most efficient solution to market failures would be to shift the burden of security onto the least-cost avoider, or the party best-suited to bear the cost—the commercial open-source consumer.[331] Many in this group, the Contributing Consumers, are already using open source responsibly. However, this group also contains the entities most culpable for introducing vulnerabilities into the open-source ecosystem: the Irresponsible Consumers.

The fact that Irresponsible Consumers generate the negative externality makes them best suited to internalize the externality; they can absorb social cost by implementing the open-source security measures that are lacking today. They are the first commercial touchpoint for the code and have exclusive control over the initial integration of open-source code into a product—they alone can identify vulnerabilities at integration. Failure to monitor in the first instance can exacerbate the risk down the supply chain;[332] the cost of addressing a vulnerable component during coding costs about one percent of replacing the same component postdeployment.[333] For these reasons, security experts have long touted the importance of shifting security left, fixing issues earlier in the supply chain.[334]

Commercial open-source consumers are also best positioned to document whichever open-source components they use, which would enable them to inform downstream customers, including other software vendors, about the

[331] *See, e.g.*, Coase, *supra* note 311.

[332] *See* Richard O. Zerbe Jr. & Howard McCurdy, *The End of Market Failure*, 23 REGUL. 10, 11–14 (2000) (describing how failure to monitor can cause inefficiencies); Sanger et al., *supra* note 184 (describing how Russian hackers exploited the vulnerabilities within one vendor's software to infiltrate upward of 250 federal agencies and businesses that all used the software).

[333] MICROSOFT & WHITESOURCE, THE COMPLETE GUIDE ON OPEN SOURCE SECURITY 12–13, https://www.mend.io/rc-content/wp/the-complete-guide-on-open-source-security-1.pdf [https://perma.cc/VGB5-F7PF].

[334] Mario Vuksan, *Shift Left Together: Coordinating a Joint Response to Supply Chain Threats*, FORBES (July 6, 2022, 8:45 AM), https://www.forbes.com/sites/forbestechcouncil/2022/07/06/shift-left-together-coordinating-a-joint-response-to-supply-chain-threats/?sh=2e57200113f1 [https://perma.cc/W4X9-VEEV]; *see also* NAT'L SEC. AGENCY, OFF. OF THE DIR. OF NAT'L INTEL. & CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, SECURING THE SOFTWARE SUPPLY CHAIN: RECOMMENDED PRACTICES GUIDE FOR DEVELOPERS ii (2022), https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF [https://perma.cc/4JX5-NAX2] ("The software supplier (vendor) is responsible for liaising between the customer and software developer. Accordingly, vendor responsibilities include ensuring the integrity and security of software via contractual agreements, software releases and updates, notifications, and mitigations of vulnerabilities.").

ingredients in their product.[335] They are uniquely capable of scanning for vulnerabilities, reporting them, determining whether they impact any given customer, and patching them. The average end-user, such as a mom-and-pop cupcake shop, lacks the capability to adopt the security measures that could find and remediate vulnerabilities. If commercial entities have the technical acumen and resources to build software, they should also be able to secure it in the long term.

Instead, Irresponsible Consumers shrug off all responsibility. First, they attempt to shift the burden of security to the open-source developer. Some are demanding volunteers comply with onerous security requirements for the chance to . . . give their software away for free?[336] Others have sought to fundamentally alter the ethos of the open-source community itself, with proposals to ban pseudonymous and anonymous project owners and maintainers in the name of security.[337] Encumbering the open-source community is as impractical as it is unfair—taxing the altruism of an underresourced community will further deplete the supply of open-source support and exacerbate the underlying problem. Second, Irresponsible Consumers attempt to shift liability for any harm arising out of their poor security practices to their customers, end-users, or third-party beneficiaries of their contracts by disclaiming all warranties regarding proprietary code and its open-source components.

Open-source defects should be governed the same way product defects are: when a defect in a product, such as a car, injures a consumer, the law holds every commercial link in the supply chain capable of having identified and remediated the defect accountable.[338] Manufacturers are expected to take on the costs of recalling the faulty product, compensating injured victims, and investing in an improved product. The average consumer can no more assess the risk profile of software than they could a faulty engine. National Cyber

[335] Hunter & De Vynck, *supra* note 86 (explaining that the best thing consumers can do is "just wait and let the experts fix their software programs" and then implement the patches once they are distributed).

[336] Jeff Geerling (@geerlingguy), TWITTER (June 30, 2022 3:24 PM), https://twitter.com/geerlingguy/status/1542589998725300229?s=21&t=qW36lPwdbt-bfR0vvt20Og [https://perma.cc/5TF9-MYXV] ("[L]ol for one of my #opensource projects, an #infosec employee at @EpicGames emailed me this questionnaire with over 100 questions and wants me to fill it out so *they* can use my freely available open source software. No.").

[337] Eric Brewer, Rob Pike, Abhishek Arya, Ann Bertucio & Kim Lewandowski, *Know, Prevent, Fix: A Framework for Shifting the Discussion Around Vulnerabilities in Open Source*, GOOGLE SEC. BLOG (Feb. 3, 2021), https://security.googleblog.com/2021/02/know-prevent-fix-framework-for-shifting.html [https://perma.cc/4U3S-FC74].

[338] *See* R.D. Hursh, Annotation, *Liability of Manufacturer or Seller for Injury Caused by Automobile or Other Vehicle, Aircraft, Boat, or Their Parts, Supplies, or Equipment*, 78 A.L.R.2d 460 (1961) ("The manufacturer's duty of reasonable care, including inspecting and testing, is fully applicable to products fabricated by another which are incorporated into the manufacturer's product.").

Director Chris Inglis has suggested that open-source vulnerabilities should be handled the same way—with the Irresponsible Consumer, not the open-source developers, absorbing the social cost.[339] This form of liability "would provide a leveling effect, addressing current information asymmetries that prevent consumers from making informed purchasing decisions and empowering them to identify and respond to negligence."[340]

However, given the lack of incentives, Irresponsible Consumers will not voluntarily assume the responsibility of least-cost avoider; they will continue to free ride. If they continue to free ride, the public will continue to bear the costs of the negative externalities that Irresponsible Consumers create. This outcome is inefficient and detrimental to all of society because the public is ill-suited to address the harms of vulnerabilities. The net harm to society can be reduced if the Irresponsible Consumer neutralizes the threat before damage is inflicted.

III. GOVERNMENT'S ROLE IN A COORDINATED, COMPREHENSIVE RESPONSE

Saying Irresponsible Consumers should pay is easy. In practice, such a solution would probably be insufficient and hard to implement. A coordinated, comprehensive response is needed to address the threat of open-source security. This part will evaluate the various tools at the government's disposal. Section A will explain that successful intervention must facilitate coordination. Section B will review the reasons current interventions are insufficient. Section C will explore additional regulatory options available to the government and compare their merits and shortcomings. This part's analysis makes clear that interventions that rely on voluntary participation have not and will not succeed.

A. *Coordination Required To Solve Market Failures*

Addressing the resource gaps in the open-source community, the information gaps in the marketplace, and the negative externalities borne by society will require extensive coordination among open source's stakeholders.[341] Coordination's challenge is its high transaction costs.[342]

[339] Simon Sharwood, *Software Patching Must Work Like Car Safety Recalls, Says US Cyber Boss*, REG. (May 13, 2022, 4:00 PM), https://www.theregister.com/2022/05/13/us_cyber_director_patching/ [https://perma.cc/3ABD-RKYM].

[340] Herr et al., *supra* note 132.

[341] Anomaly, *supra* note 266, at 109–28; Schweik & English, *supra* note 325 ("In a commons that needs to encourage contributions rather than control over-appropriation, institutional designs need to be in place to help coordinate collective action, but need to be as unobtrusive as possible.").

[342] *Cf.* Zerbe & McCurdy, *supra* note 332, at 11 ("In essence, externalities exist because the transaction costs of resolving them are too high.").

Every party impacted by insecure open-source software would need to participate in calculating the total benefits and costs of open-source, including all externalities, and in reallocating costs efficiently from the least-cost-avoider to the projects that need the most help.[343] But, coordination is expensive because any attempt would be hindered by lack of information. The manner in which positive and negative externalities manifest in the open-source ecosystem, as network effects, frustrates attempts to quantify them.[344] The open-source market is diffuse, disconnected, and large.[345] Stakeholders rarely know each other and have no ability to find each other. And, given the incentive to free ride, they have no reason to try.

B. *Interventions to Date Have Been Lacking*

Intervention is warranted when market failures are pronounced, their harms are intolerable, and they are unlikely to self-correct.[346] Intellectual property law, competition law, and consumer protection law are all attempts to remedy market failures that threaten to harm the public. Each is an example of a comprehensive solution that changes market behavior to better serve the public welfare. Government intervention in the open-source space is not similarly comprehensive and therefore fails to exert sufficient influence on market behavior.

1. Voluntary Efforts Are Insufficient

Voluntary efforts by the open-source community and its private funders are eye-opening. They demonstrate that: (1) the open-source community wants to raise minimum security standards; (2) some large technology companies recognize they must play a role in accomplishing that; and (3) the open-source community's best efforts will be met with pushback.

[343] Herbert Hovenkamp, *Marginal Utility and the Coase Theorem*, 75 CORNELL L. REV. 783, 808–10 (1990).

[344] *See* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 483 (1998) (explaining that "'network effects' refers to a group of theories clustered around the question whether and to what extent standard economic theory must be altered in cases in which 'the [u]tility that a user derives from consumption of a good increases with the number of other agents consuming the good'" (quoting Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424, 424 (1985))).

[345] Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 (emphasizing "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").

[346] *See* PIGOU, *supra* note 284, at 189–92; Samuelson, *supra* note 240, at 387–89; Assaf, *supra* note 211, at 31, 33–35. *See generally* HENRY SIDGWICK, THE PRINCIPLES OF POLITICAL ECONOMY (3d ed. 1901) (discussing general economic theory and the government's role in improving the market).

The open-source community, including its private sector investors, is aware of its security problem. In fact, they are already attempting to build out institutions and standards to secure open source. For example, the Open Source Security Foundation ("OpenSSF") has already met with the White House twice and has ten dedicated workstreams all focused on securing the open-source ecosystem.[347] It has even begun to develop a free, comprehensive open-source curriculum to fill the cybersecurity workforce gap and provide necessary training regarding the nuances of open source.[348] The Open Source Technology Improvement Fund ("OSTIF") was recently founded to provide free security auditing services to open-source projects and continues to grow.[349] These efforts seek to establish minimum security standards, improve information sharing, and encourage resource contributions from vendors. OSTIF reports it requires a total of $2.3 million per year to scale its service delivery to meet demand.[350] Currently, it is dependent on fundraising.[351]

However, progress has been incremental—and insufficient. First, these nonprofits primarily represent open source's Contributing Consumers; many noncorporate contributors, such as individual volunteer developers, are absent in these efforts. Second, corporate participation is voluntary so other market players can free ride, resulting in underinvestment of the effort. Even the Contributing Consumers that have donated have not pledged enough money for OpenSSF to achieve its goal. OpenSSF estimated that implementation of its strategy will cost $147.9 million over two years[352]—for context, the 2022

[347] THE LINUX FOUND. & OPEN SOURCE SEC. FOUND., THE OPEN SOURCE SOFTWARE SECURITY MOBILIZATION PLAN 5–11, https://openssf.org/oss-security-mobilization-plan/ (click "Read the Plan") [https://perma.cc/M5WV-LAJ4].

[348] david-a-wheeler, *Secure Software Development Fundamentals*, GITHUB (Nov. 20, 2022), https://github.com/ossf/secure-sw-dev-fundamentals/blob/main/secure_software_development_fundamentals.md [https://perma.cc/83SK-73N3].

[349] OPEN SOURCE TECH. IMPROVEMENT FUND, https://ostif.org/ [https://perma.cc/M96D-PFWL].

[350] Amir-Montazery, *Securing Critical Projects Managed Audit Program Initiative - Proposal*, GITHUB (Oct. 13, 2021), https://github.com/ostif-org/OSTIF/blob/main/Managed%20Audit%20Program/Proposal.md [https://perma.cc/2VAF-J39T] ("At approximately $2.3 million, OSTIF can work exclusively on projects and forward-looking strategy without spending time and resources on fundraising activities. . . . OSTIF is formulated to be able to scale with funding in order to build an adaptive permanent organization. With committed long-term funding, OSTIF can hire additional staff and greatly expand the number of projects that can be completed each year.").

[351] See *Our Mission*, OPEN SOURCE TECH. IMPROVEMENT FUND, https://ostif.org/the-ostif-mission [https://perma.cc/ZG8V-E4WA] (describing how OSTIF relies on "public fund-raising and the solicitation of donations from corporate and government donors").

[352] THE LINUX FOUND. & OPEN SOURCE SEC. FOUND., *supra* note 347, at 12; *see also* Press Release, OpenSSF, The Linux Foundation and Open Source Software Security Foundation (OpenSSF) Gather Industry and Government Leaders for Open Source Software Security Summit II

infrastructure bill appropriated $65 billion for broadband, another example of infrastructure that bears the qualities of a public good.[353] So far, certain Contributing Consumers like Microsoft and Google have pledged $30 million to support OpenSSF's efforts.[354] The remaining sum, and all future security efforts, would impose a small burden on market players if distributed efficiently, and society at large would be made better off for the investment.

On its own, the open-source community does not have the leverage to enact necessary changes. This past year, two of the largest open-source registries announced that they will impose minimum security measures on "critical" projects, as defined by popularity.[355] Maintainers of "critical" projects, including hobbyists and paid developers, must secure their accounts with two-factor authentication ("2FA") to continue contributing to the project. This simple measure could prevent 99.9% of account-takeovers, a rising threat to open-source security.[356] However obvious this measure seems, the new requirement resulted in an outcry from community members particularly averse to top-down mandates—authors of extremely popular projects threatened to abandon their posts, which could potentially break the systems of any end-user reliant on their projects.[357] With GitHub slated to roll out mandatory 2FA for all its developers by the end of 2023, we can expect more resistance.[358]

(May 12, 2022), https://openssf.org/press-release/2022/05/12/the-linux-foundation-and-open-source-software-security-foundation-openssf-gather-industry-and-government-leaders-for-open-source-software-security-summit-ii/ [https://perma.cc/D5YU-QN33].

[353] *Fact Sheet: The Bipartisan Infrastructure Deal*, WHITE HOUSE (Nov. 6, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/06/fact-sheet-the-bipartisan-infrastructure-deal/ [https://perma.cc/YH8E-TEJ7].

[354] Carly Page, *Tech Giants Pledge $30M To Boost Open Source Software Security*, TECHCRUNCH (May 16, 2022, 9:58 AM), https://techcrunch.com/2022/05/16/white-house-open-source-security/ [https://perma.cc/VL9S-4TD2]; *cf. Top Companies Contributing to Open Source – 2011/2021*, *supra* note 105 (listing the top companies contributing code, not monetary contributions, to open source).

[355] *See* Betty Li, *Making Popular Ruby Packages More Secure*, RUBYGEMS BLOG (June 13, 2022), https://blog.rubygems.org/2022/06/13/making-packages-more-secure.html [https://perma.cc/Y6UU-GJUX]; *PyPI 2FA Security Key Giveaway*, PYPI, https://pypi.org/security-key-giveaway/ [https://perma.cc/ZR6S-W753].

[356] Melanie Maynes, *One Simple Action You Can Take To Prevent 99.9 Percent of Attacks on Your Accounts*, MICROSOFT (Aug. 20, 2019), https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ [https://perma.cc/TJ5M-RKTX].

[357] James Bennett, *Yes, I Have Opinions on Your Open Source Contributions*, B-LIST (July 11, 2022), https://www.b-list.org/weblog/2022/jul/11/pypi/ [https://perma.cc/9VEF-PMGX]; Armin Ronacher, *Congratulations: We Now Have Opinions on Your Open Source Contributions*, ARMIN RONACHER'S THOUGHTS & WRITINGS (July 9, 2022), https://lucumr.pocoo.org/2022/7/9/congratulations/ [https://perma.cc/B6GZ-GMPR].

[358] *See* Mike Hanley, *Software Security Starts with the Developer: Securing Developer Accounts with 2FA*, GITHUB BLOG (May 4, 2022), https://github.blog/2022-05-04-software-security-starts-with-the-developer-securing-developer-accounts-with-2fa/ [https://perma.cc/KU4B-86HE].

The open-source community acknowledges it cannot secure open source on its own. First, the developer community's resistance to basic security measures suggests that the new automated tools organizations have built to facilitate more complex security measures may not see widespread adoption.[359] Second, the adoption of these policies is also hamstrung by resource deficiencies. While GitHub might have the resources to mandate 2FA for all its users, other less-resourced entities do not.[360] Third, changes in the open-source community can only go so far. The Irresponsible Consumers must also adopt these security practices and use the available tools but, given they are voluntary, they are unlikely to do so.[361]

Researchers have called for targeted investments from government[362] and consumers of open-source projects[363] to fund more full-time maintainers for important projects and entities offering open-source security services for free. The open-source community has requested upstream contributions from *all* its consumers—support in the form of code-review and improvement.[364] While some companies have risen to the occasion, the vast majority have not.

[359] *See* Lily Hay Newman, *GitHub Moves To Guard Open Source Against Supply Chain Attacks*, WIRED (Aug. 8, 2022, 7:19 PM), https://www.wired.com/story/github-code-signing-sigstore/ [https://perma.cc/N3WU-NXB5] ("GitHub, which itself is owned by Microsoft, announced on Monday that it plans to support code signing, a sort of digital wax seal, for npm software packages using the code-signing platform Sigstore."); Ericka Chickowski, *We Have the Tech To Scale Up Open Source Vulnerability Fixes – Now It's Time To Leverage It*, DARKREADING (Aug. 8, 2022), https://www.darkreading.com/dr-tech/we-have-the-tech-to-scale-up-open-source-vulnerability-fixes-now-it-s-time-to-leverage-it [https://perma.cc/Y8R2-AM5W] (arguing that the technology to bulk fix vulnerabilities exists but it lacks adoption and investment).

[360] The two aforementioned registries, for example, do not have the support staff required to field the deluge of account reset requests that would be inevitable if all users were required to implement 2FA. *See* Li, *supra* note 355.

[361] *See* Yu, *Open Source Security Needs Automation*, *supra* note 181 (highlighting the fact that "most companies saw cybersecurity as a cost and would not want to address it actively in the absence of any incentive"). *But see* Ron Miller, *Group of Security Companies Launches Open Source Project To Ease Data Sharing*, TECHCRUNCH (Aug. 10, 2022, 12:45 PM), https://techcrunch.com/2022/08/10/group-of-security-companies-launches-open-source-project-to-ease-data-sharing/ [https://perma.cc/9HBX-4EPM] (describing a voluntary coalition of the biggest technology and security companies to develop and commit to using interoperable security tools for improved data sharing).

[362] Ashwin Ramaswami, *Securing Open Source Software at the Source*, PLAINTEXT GRP. (June 11, 2021), https://www.plaintextgroup.com/reports/securing-open-source-software-at-the-source [https://perma.cc/45ZG-4X32].

[363] Herr et al., *supra* note 132.

[364] *Responding to and Learning from the Log4Shell Vulnerability: Hearing Before the S. Comm. On Homeland Sec. & Governmental Affs.*, 117th Cong. (2022) (opening statement of David Nalley, President, Apache Software Foundation), https://www.hsgac.senate.gov/hearings/responding-to-and-learning-from-the-log4shell-vulnerability/ [https://perma.cc/47LQ-N9MJ]; *see* dominictarr, *Statement on Event-Stream Compromise*, *supra* note 134 (showing an experienced open-source maintainer advocating for payment to maintainers and upstream code contributions).

2. Government Interventions Are Piecemeal

Securing open source is not just a matter of investing in a few projects here and there; it entails overhauling the existing software development lifecycle and redesigning it to include security checks for open source every step of the way. Despite recognizing the existential threat posed by insecure open-source software, the government's response has been tepid so far.[365]

a. Limited Scope

Most of the government's interventions addressing software security focus on federal systems. In 2014, the government passed the Federal Information Security Modernization Act ("FISMA"), which directed the U.S. Department of Homeland Security ("DHS") to establish cybersecurity policies for federal agencies.[366] In executing the directive, DHS found its efforts were impeded by vendor constraints.[367] However, in the intervening years, the government did little more than incrementally adjust its cybersecurity policies.[368]

The private sector remained unaddressed until 2021, when the White House issued an executive order ("EO") addressing the software supply chain.[369] This order explicitly addressed the private sector, requiring those companies selling to the federal government to take precautionary measures to identify and remediate vulnerabilities in their software. It also specifically addressed open-source security, calling on the National Institute of Standards and Technology ("NIST") to establish federal software procurement guidelines.[370] The ensuing NIST guidelines confirm that open source *managed*

[365] Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 ("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.").

[366] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 3553, 128 Stat. 3073, 3075 (codified as amended at 44 U.S.C. § 3553 (2021)) (empowering DHS to evaluate and enforce compliance with 2003 FISMA, which required agencies to develop concrete cybersecurity policies and abide by them).

[367] U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-133, INFORMATION TECHNOLOGY: DHS DIRECTIVES HAVE STRENGTHENED FEDERAL CYBERSECURITY, BUT IMPROVEMENTS ARE NEEDED 17 (2020).

[368] *See, e.g.*, Exec. Order No. 13,636, 78 Fed. Reg. 11739, 11739 (Feb. 12, 2013) (resulting in the creation of a cybersecurity framework that is voluntary and unenforceable); Exec. Order No. 14,028, 86 Fed. Reg. 26633, 26633 (May 12, 2021). *See generally* JON BOYENS, ANGELA SMITH, NADYA BARTOL, KRIS WINKLER, ALEX HOLBROOK & MATTHEW FALLON, NAT'L INST. OF STANDARDS & TECH. & U.S DEP'T OF COM., NIST SP 800-161r1, CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT PRACTICES FOR SYSTEMS AND ORGANIZATIONS (2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf [https://perma.cc] (updating NIST software supply chain guidance, which remains voluntary for the private sector).

[369] Exec. Order No. 14,028, 86 Fed. Reg. at 26637–41.

[370] *Id.* at 26637–38.

by the government could be considered critical infrastructure software subject to the EO's requirements.[371] However, the EO's treatment of open source pales in comparison to the expectations of vendors vis-à-vis their closed-source applications.[372]

The EO is not without teeth though; recent guidance has indicated that vendors will be required to attest to their adoption of secure development practices for all software sold to the federal government, including renewals and major releases, or subject themselves to third-party review by a certified assessor, thereby exposing them to liability for failure to comply with those attestations.[373]

The EO's most direct mandate was a requirement that software vendors provide agency customers with a Software Bill of Materials ("SBOM") enumerating the various software components, including open-source components, contained in their products.[374] The requirement makes progress towards bridging the information divide between software vendors and their customers. To comply with this mandate, companies must analyze each of their

[371] NAT'L INST. OF STANDARDS & TECH., SOFTWARE SUPPLY CHAIN SECURITY GUIDANCE UNDER EXECUTIVE ORDER (EO) 14028 SECTION 4E, at 2 (2022), https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf [https://perma.cc/6GBE-UL9C] (excluding "open-source software freely and directly obtained by federal agencies" from the scope of its security recommendations). *See generally Software Security in Supply Chains: Open Source Controls*, NIST, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-open [https://perma.cc/JZB7-FS2V] (dedicating a single page to open-source software in response to the EO's directive to establish open-source security recommendations); NAT'L INST. OF STANDARDS & TECH., DEFINITION OF CRITICAL SOFTWARE UNDER EXECUTIVE ORDER (EO) 14,028 (2021), https://www.nist.gov/system/files/documents/2021/10/13/EO%20Critical%20FINAL.pdf [https://perma.cc/6558-MEVL] (laying out NIST's approach and current definition for "EO-critical software").

[372] Regarding open-source software, the Executive Order calls on NIST to establish guidelines that hold vendors responsible for "ensuring and attesting, *to the extent practicable*, to the integrity and provenance of open source software used within any portion of a product." Exec. Order No. 14,028, 86 Fed. Reg. 26633, 26639 (May 17, 2021) (emphasis added). Regarding their proprietary software, the guidelines hold vendors responsible for more: "[M]aintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis." *Id.* at 26638. It is arguable that the latter provision, which specifically addresses open-source software, is a gloss on the general expectations of software vendors laid out in the former. However, canons of interpretation counsel against assuming that redundancy. Additionally, the qualifying language "to the extent practicable" does not exist in the former section, suggesting the Executive Order intentionally creates separate expectations for open-source software that are subject to their own lower standard.

[373] Memorandum from Shalanda D. Young, Dir., Off. of Mgmt. & Budget, Exec. Off. of the President to Heads of Exec. Dep'ts & Agencies, M-22-18 (Sept. 14, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf [https://perma.cc/QJV3-4QRS].

[374] Exec. Order No. 14,028, 86 Fed. Reg. at 26638.

products to identify their components and map their dependencies—providing insight into the Russian doll that is modern software.[375] Irresponsible Consumers that previously neglected to document the open-source components they use will have to improve their security practices if they hope to sell to the government. Failing to provide accurate, up-to-date SBOMs not only risks losing valuable government clients, but it also exposes companies to liability.

The process of building and distributing SBOMs will improve software security.[376] Without them, even the largest, most sophisticated technology companies had to deploy hundreds of employees over several weeks to simply identify where they were vulnerable to attack, let alone patch each of those components.[377] By providing detailed information about the components in software sold to the government, SBOMs help agencies identify where a reported vulnerability is in their system, increasing the speed with which they can fix the issue. By equipping agencies with insight into the components in the software they use, SBOMs empower agency customers to put upward pressure on software vendors to improve their security practices.

But these requirements are only for federal contractors.[378] For the rest of the industry, government regulations remain voluntary.[379] This includes the wide array of private sector entities that may not sell software to the government but still supply software containing open source to entities delivering critical functions. An investigation of the impact of these cybersecurity frameworks in critical infrastructure industries found that the voluntary nature of the framework presented a challenge to the impact of the framework on industry.[380] NIST itself noted that, while best practices for software supply chain are emerging, there remains no de facto standard and that

[375] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-105103, CRITICAL INFRASTRUCTURE PROTECTION: AGENCIES NEED TO ASSESS ADOPTION OF CYBERSECURITY GUIDANCE 1 (2022), https://www.gao.gov/assets/gao-22-105103.pdf [https://perma.cc/EU8A-7WTM].

[376] *See* Joseph Marks, *An 'Ingredients List' for Software Could Help Prevent the Next Log4j*, WASH. POST (Jan. 26, 2022, 7:32 AM), https://www.washingtonpost.com/politics/2022/01/26/an-ingredients-list-software-could-help-prevent-next-log4j/ [https://perma.cc/SS85-HH5E] [hereinafter Marks, *An 'Ingredients List'*] ("One big idea being pushed by government cyber officials is a Software Bill of Materials (SBOM)—an ingredients list for tech systems that organizations can consult when a new bug is discovered to see if they have vulnerable software needing to be patched.").

[377] Hunter & De Vynck, *supra* note 86 ("At Google alone, more than 500 engineers had been going through reams and reams of code to make sure it was safe, according to one employee.").

[378] Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 ("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.").

[379] *Id.*

[380] *See* Marks, *An 'Ingredients List,' supra* note 376.

none of the existing frameworks are individually comprehensive.[381] In such an uncertain landscape, compliance is difficult and Irresponsible Consumers are unlikely to take on the challenge.[382] As long as these requirements are only for federal contractors, their impact on the broader open-source ecosystem and critical infrastructure specifically will be limited.[383]

Further, the SBOM mandate, even if expanded to the private sector, is not enough. A list of ingredients cannot tell a customer which ingredient is safe. Comparable to a list of ingredients on a snack or medication you purchase, the information is only as useful as your ability to parse it. By failing to provide any vulnerability information, SBOMs shift the burden of evaluating risk onto the customer. To operationalize an SBOM, a company must be able to read it (which is a challenge, as there is no mandated standard format for an SBOM) and actually use it to check databases, such as the National Vulnerability Database[384] or the Known Exploited Vulnerability Catalog,[385] for new vulnerabilities found in the software components the SBOM lists.[386] These

[381] NIST SSDF, Google SLSA, Gartner, Mitre & OWASP, *Cybersecurity Frameworks & Standards for Securing Software Supply Chains*, CYCODE, https://cycode.com/security-frameworks-and-standards/ [https://perma.cc/KJ7L-YC25].

[382] SBOM champion Allan Friedman hopes that one day, SBOMs will be a regular part of everyday life—a standard industry practice, like tax reporting. Kyle Alspach, *The White House Wants New Transparency into Software Components. The Security Benefits Won't Arrive Quickly*, PROTOCOL (Aug. 25, 2022), https://www.protocol.com/enterprise/biden-sbom-open-source-software [https://perma.cc/KWP3-9PPL] [hereinafter Alspach, *The White House Wants New Transparency*]. However, tax reporting is ubiquitous because it is mandatory and enforceable with severe penalties. Without aggressive incentives, companies are unlikely to adopt widespread SBOM distribution. *Preventing Supply Chain Attacks Like SolarWinds*, LINUX FOUND. (Jan. 13, 2021), https://www.linuxfoundation.org/blog/blog/preventing-supply-chain-attacks-like-solarwinds [https://perma.cc/2VYY-VU85] (arguing that companies are likely unwilling to share SBOM data voluntarily but that users need to demand this information from private sector vendors to avoid devastating attacks like Solarwinds).

[383] Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 ("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.").

[384] Beck Bracken, *Google: SBOMs Effective Only if They Map to Known Vulns*, DARKREADING (June 14, 2022), https://www.darkreading.com/vulnerabilities-threats/sboms-only-effective-if-they-map-to-k'own-flaws [https://perma.cc/69UK-V2L2] ("But Google's Open Source Security Team points out in a blog post today that SBOM use alone isn't an effective tool for assessing exposure. Rather, the documentation should be compared with a database of known vulnerabilities to identify any known software flaws."); *see also National Vulnerability Database*, NIST, https://nvd.nist.gov/ [https://perma.cc/L97V-R89Q].

[385] *Known Exploited Vulnerability Catalog*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/known-exploited-vulnerabilities-catalog [https://perma.cc/X34S-MBS4].

[386] In the spring of 2022, CISA issued guidance recommending that software vendors build a Vulnerability Exploitability eXchange ("VEX") document that would be able to inform customers proactively whether the product they were sold contains a vulnerability that requires a patch. It remains

activities are costly and cumbersome given the nature of open source, so many companies might not undertake them.

While most Contributing Consumers, such as Google and Intel, might have the resources and security maturity to demand machine-readable SBOMs and regularly scan databases for new vulnerabilities that impact their systems, there are countless small businesses using open source that cannot.[387] Some experts say the software needed to analyze SBOMs in bulk and glean insights from the data do not yet exist.[388] These small businesses have no option but to trust their vendor. They are the companies that drive the high number of both outstanding critical vulnerabilities and average days to patch. One study found that forty-three percent of all cyberattacks target small to medium-sized businesses[389] and that only forty percent of small businesses have an actionable open-source policy.[390]

Legislative efforts to address open source head-on regularly fail. The House version of the 2022 National Defense Authorization Act included funding for a dedicated open-source security center within DHS,[391] but the

voluntary. *See generally* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, VULNERABILITY EXPLOITABILITY EXCHANGE (VEX) – USE CASES (2022), https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Aprill2022.pdf [https://perma.cc/C6VW-5FDK] (describing guidelines for security advisories sent out in the event of a vulnerability).

[387] *See* Yu, *Open Source Security Needs Automation*, *supra* note 181 ("Identifying all passive and indirect interdependencies was far from easy, he noted, adding that it could be difficult for companies to access security experts to carry out such works. He pointed to the need for automated tools to support such security assessments."); Geller, *Lesson from Log4j*, *supra* note 121 ("[F]ew companies maintain accurate and comprehensive inventories of their software or possess the technology to automatically process the ingredient lists.").

[388] Alspach, *The White House Wants New Transparency*, *supra* note 382 ("Even the much-touted use case of checking the SBOM for a flaw like Log4Shell is not something even a skilled developer would want to do manually, and it's beyond the reach of anyone non-technical, said Gareth Rushgrove, vice president of products at Snyk, which offers developer security tools including SBOM generation. Notably, in the initial stage, an SBOM won't be automatically correlated with vulnerability information."). *But see* Danesh Kumar Badlani & Adrian Diglio, *Microsoft Open Sources Its Software Bill of Materials (SBOM) Generation Tool*, MICROSOFT (July 12, 2022), https://devblogs.microsoft.com/engineering-at-microsoft/microsoft-open-sources-software-bill-of-materials-sbom-generation-tool/ [https://perma.cc/9RJ8-AUWF] ("Open sourcing our SBOM tool is an important step towards fostering collaboration and innovation within our community, and we believe this will enable more organizations to generate SBOMs as well as contribute to its development.").

[389] Scott Steinberg, *Cyberattacks Now Cost Companies $200,000 on Average, Putting Many Out of Business*, CNBC (Mar. 9, 2020, 11:37 AM), https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html [https://perma.cc/8W3W-6BGV].

[390] *See* HENDRICK & MCKEAY, *supra* note 21, at 6 (reporting that only forty-one percent have an open-source policy that they know exists, a prerequisite for a policy to be actionable).

[391] Aaron Schaffer, *Defense Bill Is a Major Cyber Legislation Opportunity for Rep. Langevin*, WASH. POST (June 21, 2022, 7:36 AM), https://www.washingtonpost.com/politics/2022/06/21/defense-bill-is-major-cyber-legislation-opportunity-rep-langevin/ [https://perma.cc/PDG2-4LSM (dark archive)].

funding did not make it into the final bill.[392] At the state level, New York has failed to pass a bill to give individuals and organizations tax credit for open-source contributions every year for thirteen years now.[393] In fact, such a bill has never gotten out of committee.[394]

At the federal level, the Senate Homeland Security Committee recently approved, with no markup, legislation to secure open-source software.[395] The bill directs CISA to hire open-source experts "to the greatest extent practicable," to publish a framework on open-source code risk, to perform an actual assessment of open-source components in federal networks, to automate the assessment tool to the degree practicable, and to study whether the framework could be applied to critical infrastructure outside the government.[396] It also establishes a pilot program to create open-source program offices at federal agencies.[397]

However, the bill falls short in several ways. Agencies have a poor track record of adopting minimum cybersecurity measures. The fourteenth Federal Information Technology Acquisition Reform Act ("FITARA") scorecards showed that only one of the twenty-four agencies received an A in implementing satisfactory technology acquisition, management, and security practices.[398] Eleven agencies received a C+, with eight agencies seeing a score decrease from the previous year.[399] With no reason to believe agencies will be of much help, it is wishful to think CISA can inventory and evaluate the federal government's systems for open-source security singlehandedly with no additional budget to hire outside help. To think CISA can accomplish this within a year of actually developing the framework is patently unreasonable. Even larger shortcomings are the lack of funding support for the open-source community, the failure to conscript the private sector's support, and the absence of any mandates that private critical infrastructure entities conduct their own internal audits. At best, the bill encourages CISA to *study* opportunities to apply the framework to the private sector, using data from *voluntary* participants in

[392] Nagle, *Strengthening Digital Infrastructure*, *supra* note 7.

[393] *Id.*

[394] *Id.*

[395] Martin Matishak, *Senate Panel Approves Open-Source Software Bill, Though Future Unclear*, RECORD (Sept. 28, 2022), https://therecord.media/senate-panel-approves-open-source-software-bill-though-future-unclear/ [https://perma.cc/WR6X-64FZ].

[396] Securing Open Source Software Act of 2022, S. 4913, 117th Cong. § 2220E(b)–(c) (2022).

[397] *Id.* § 5(c)(1).

[398] Chris Riotta, *FITARA 14 Sees Just One Overall A and Stagnant Grades*, FCW (July 28, 2022), https://fcw.com/it-modernization/2022/07/fitara-14-sees-just-one-overall-and-stagnant-grades/375049/ [https://perma.cc/587B-NLBY].

[399] *Id.*

critical infrastructure industries.[400] As discussed above and explored further below, reliance on voluntary participation is misguided.

There is hope, though, that the current administration's software security goals are broader and stronger than the initiatives we have seen so far. The administration announced its much-anticipated national cyber strategy in March 2023.[401] The new policy echoes the very policy changes proposed in this paper, stating that "[r]esponsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product."[402] Further, the strategy calls on Congress to "develop legislation establishing liability for software products and services" to "prevent manufacturers and software publishers with market power from fully disclaiming liability by contract, and establish higher standards of care for software in specific high-risk scenarios."[403] And the policy backs mandatory requirements: "While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements" has too often resulted in inconsistent and, in many cases inadequate, outcomes.[404] If the administration is able to marshal congressional and interagency support, its vision may make unprecedented progress in securing digital critical infrastructure. Implementation aside, the cyber plan's focus on "realign[ing] incentives to favor long-term investments in security, resilience, and promising new technologies," enshrines the very conclusions this Article draws in national policy and is cause for optimism.[405]

b. Limited Enforceability

Beyond regulations, the government has hinted at the possibility of enforcement. Since the Log4Shell incident, the Federal Trade Commission ("FTC") has threatened companies that are slow to implement patches with enforcement actions.[406] Consumer protection law can be a powerful tool and, with these threats, the FTC has signaled an interest in expanding its

[400] *See* S. 4913 § 3(a)(3).

[401] *See* THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 1 (Mar. 1, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/6R7Q-8BEW].

[402] *Id.* at 21.

[403] *Id.*

[404] *Id.* at 8.

[405] *Id.* at i.

[406] *See FTC Warns Companies To Remediate Log4j Security Vulnerability*, FED. TRADE COMM'N (Jan. 4, 2022), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability [https://perma.cc/6FCS-JTK6].

enforcement of consumer protection laws against software and internet platforms. Companies proactively change their behavior in anticipation of FTC action. Indeed, many companies voluntarily adapt their behavior to comply with consent decrees levied against competitors to avoid enforcement actions themselves.

However, the FTC cannot be the bulwark of government effort to secure the open-source ecosystem. It lacks the manpower and arguably, the technical acumen. It has made valiant efforts to hold companies accountable for poor security practices in the past with limited success. Most notably, the Equifax hack, which compromised the personal information of nearly 150 million Americans, was courtesy of an *unpatched* open-source vulnerability.[407] The FTC took immediate action but, even so, many complain that the consequences were not nearly severe enough.[408] Additionally, while FTC efforts can have positive ripple effects, they cannot guarantee industry-wide impact. Despite the substantial penalty against Equifax, other companies failed to patch the very same vulnerability in their popular products.[409]

Thousands of devices remain vulnerable to Log4Shell and companies on average take ninety-eight days to fix a vulnerability—sixty days to fix a critical vulnerability.[410] This shows that existing enforcement actions are too little, too late, in the software lifecycle. Security requirements remain entirely voluntary for companies that do not sell to the federal government, doing little to change the behavior of Irresponsible Consumers introducing risk into the ecosystem. And none of the requirements do anything to address the lack of support for the open-source community on whom open-source software security depends.

[407] *See* Alfred Ng, *How the Equifax Hack Happened, and What Still Needs To Be Done*, CNET (Sept. 7, 2018, 4:54 AM), https://www.cnet.com/news/privacy/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/ [https://perma.cc/EFR9-967E].

[408] *See* Zack Whittaker, *A Year Later, Equifax Lost Your Data but Faced Little Fallout*, TECHCRUNCH (Sept. 8, 2018, 9:00 AM), https://techcrunch.com/2018/09/08/equifax-one-year-later-unscathed/ [https://perma.cc/4EXQ-AL7Q]. Equifax eventually agreed to a $425 million settlement in September 2022. *Equifax Data Breach Settlement*, FED. TRADE COMM'N (Dec. 2022), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement [https://perma.cc/54BH-KT78].

[409] Lucian Constantin, *Zero-Day Flaw in Atlassian Confluence Exploited in the Wild Since May*, CSO ONLINE (July 4, 2022, 2:00 AM), https://www.csoonline.com/article/3662755/zero-day-flaw-in-atlassian-confluence-exploited-in-the-wild-since-may.html [https://perma.cc/ZXP7-942T] (describing the same open-source vulnerability, for which a patch exists, being found in other companies' products).

[410] PERKAL, *supra* note 31, at 2; Newman, *Log4j Vulnerability*, *supra* note 31; EDGESCAN, 2022 VULNERABILITY STATISTICS REPORT 11 (2022), https://www.edgescan.com/ [https://perma.cc/A94A-WCE2 (staff-uploaded archive)] (click "Intel Hub" and choose "Stats Reports" from dropdown).

C. *Tools for a More Effective Response to Open-Source Security*

Protecting critical infrastructure requires designing an institutional framework that would address adverse incentives, bridge the information divide, ensure efficient resource allocation, and enforce minimum standards. This section begins by explaining that these efforts must start with designating open source as critical infrastructure. This section proceeds to evaluate the additional tools that can enhance the benefits of a critical infrastructure designation.

1. Designate Open Source as Critical Infrastructure

Designating open-source development as a critical infrastructure subsector and its maintenance as a National Critical Function would elevate the resource's status, afford it the benefits of government support, and ensure its voice is brought to the table for discussions related to the protection of critical infrastructure. Although not all open-source projects are critical per se, granting the resource critical infrastructure status would open the door for government identification of the most critical open-source projects in the ecosystem.

As critical infrastructure, open source would benefit from government efforts to protect critical infrastructure assets and build their resilience.[411] The former focuses on taking measures to harden critical functions preventively and responsively to avoid their being taken offline. The latter focuses on contingency planning and long-term investments in future preparedness, including supporting asset maintenance, incentivizing secure practices, and identifying assets that could serve as substitutes or support during a crisis.[412] Underlying these goals is an intention to encourage enterprises to invest in security beyond what their individual cost-benefit analyses would justify.[413]

As critical infrastructure, the government would direct its efforts towards identifying and prioritizing critical open-source projects for inclusion in a

[411] *See* CONG. RSCH. SERV., REP. NO. 45809, CRITICAL INFRASTRUCTURE: EMERGING TRENDS AND POLICY CONSIDERATIONS FOR CONGRESS 5 (2019).

[412] *See, e.g.*, DHS, *HIFLD*, *supra* note 228 (providing access to national foundation-level geospatial data with the open public domain to support community preparedness, resiliency, and research).

[413] The 2013 NIPP states that "[g]overnment can succeed in encouraging industry to go beyond what is in their commercial interest and invest in the national interest through active engagement in partnership efforts." DEP'T OF HOMELAND SEC., NIPP 2013: PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE 1–2 (2013) [hereinafter NIPP 2013], https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf [https://perma.cc/8RHZ-S8UX].

centralized database.[414] Prioritized open-source projects would be nominated by state homeland security agencies, with input from the private sector, and reviewed by DHS before inclusion into an annually updated DHS database.[415] If successful, this effort would make substantial progress in bridging open-source's information gaps. In the past, this effort has been hampered by a lack of participation,[416] an incomplete approach in defining a critical asset,[417] and a lack of standardization in the definition of a critical asset.[418] To avoid the same outcomes for open source, it would be essential to coerce participation from the private sector, either through incentives or mandates; involve the open-source community, which has better insight into the ecosystem than any one user; and ensure asset identification efforts include critical dependencies that play a supporting role and not just the projects that seem immediately important.

Ultimately, the greatest barrier to this effort is the fact that the government prohibits treating commercial information technology providers as critical entities, which forecloses the possibility of including software products and services in a critical asset database.[419] However, given that open source is no more than a component in commercial information technology and not

[414] *See* THE WHITE HOUSE, THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS 24 (2003), https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf [https://perma.cc/8R9C-PRN8] (requiring establishment of critical asset database); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 282–83 (codified at 6 U.S.C. §§ 101–1185 (2007)) (requiring annual updates and providing in legislation a narrower, more detailed definition of critical infrastructure).

[415] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-104279, CRITICAL INFRASTRUCTURE PROTECTION: CISA SHOULD IMPROVE PRIORITY SETTING, STAKEHOLDER INVOLVEMENT, AND THREAT INFORMATION SHARING 18–20 (2022) [hereinafter GAO-22-104279].

[416] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-791T, CRITICAL INFRASTRUCTURE PROTECTION: DHS HAS MADE PROGRESS IN ENHANCING CRITICAL INFRASTRUCTURE ASSESSMENTS, BUT ADDITIONAL IMPROVEMENTS ARE NEEDED 13–14 (2016) (finding that state governments were opting not to cooperate).

[417] *See* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY: FISCAL YEAR 2017 REPORT TO CONGRESS 4 (2019) [hereinafter CISA, FY2017 REPORT TO CONGRESS], https://www.dhs.gov/sites/default/files/publications/cisa_-_improving_critical_infrastructure_cybersecurity.pdf [https://perma.cc/FP77-US3M] ("Critical infrastructure protection efforts generally have focused on assets and organizations while insufficiently accounting for the underlying services and functions.").

[418] In one instance, a petting zoo was identified as a critical asset. OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG-06-40, PROGRESS IN DEVELOPING THE NATIONAL ASSET DATABASE 11 (2006). These inconsistencies persist. *See* GAO-22-104279, *supra* note 415, at 17–18 (finding the list inconsistent, incomplete, and, to many DHS officials, useless). In response, DHS instituted the National Critical Infrastructure Prioritization Program to update the database according to a new definition. *See* Implementing Recommendations of the 9/11 Commission Act of 2007 § 1001.

[419] Exec. Order No. 13,636, 78 Fed. Reg. 11739, 11742 (Feb. 12, 2013) (ordering that DHS "shall not identify any commercial information technology products or consumer information technology services under this section" as critical entities).

commercial by itself, particularly important projects can arguably be included in the database under this rule.

Critical infrastructure designation can trigger government prioritization for support delivery, such as on-site risk assessments, administration of regulatory regimes, and emergency preparedness and response coordination, among other activities.[420] The list of critical assets is used to inform the distribution of preparedness grants to states.[421] Critical infrastructure entities benefit from access to federal cyber risk assessment resources, threat information sharing programs, classified national security information, incident response support, cross-sector emergency readiness plans, and the ability to influence policy.[422] For open source, this can mean access to much-needed funding as well as threat information and cross-sector coordination that can inform resource allocation and direct limited maintenance support. Because "covered" critical infrastructure entities using open source are already required to report cyber incidents, the open-source community can learn about vulnerabilities that impact their projects and other users from that privately disclosed information, as long as they are at the table.[423]

Critical infrastructure designation can also serve as a public signal, bringing open source into the national spotlight and raising awareness regarding the issue of open-source security. For example, after Russia attempted to interfere in the United States' 2016 election by exploiting its election systems,[424] the government designated election assets and entities as critical

[420] CONG. RSCH. SERV., REP. NO. 45809, CRITICAL INFRASTRUCTURE: EMERGING TRENDS AND POLICY CONSIDERATIONS FOR CONGRESS 7 (2019).

[421] GAO-22-104279, *supra* note 415, at 22.

[422] *Sector Risk Management Agencies*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/sector-risk-management-agencies [https://perma.cc/G2US-FQ7Y]; *see* CISA, FY2017 REPORT TO CONGRESS, *supra* note 417, at 4; NIPP 2013, *supra* note 413, at 1–2. *See generally* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, NATIONAL CRITICAL FUNCTIONS: AN EVOLVED LENS FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2019) [hereinafter CISA, NATIONAL CRITICAL FUNCTIONS], https://www.cisa.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf [https://perma.cc/7RW4-ZG98] (summarizing national critical functions).

[423] *See* Cyber Incident Reporting for Critical Infrastructure Act, Pub. L. No. 117-103, §§ 2241(a)(6), 2242(a), 136 Stat. 1038, 1041–44 (2022) (codified at 6 U.S.C. §§ 681a, 681b (2022)).

[424] *See* Greg Jaffe & Craig Timberg, *Russian Interference in 2016 Sets Landscape for 2020 Presidential Campaign*, WASH. POST (Apr. 19, 2019, 3:03 PM), https://www.washingtonpost.com/politics/russian-interference-in-2016-sets-landscape-for-2020-presidential-campaign/2019/04/19/089dacde-6231-11e9-9ff2-abc984dc9eec_story.html [https://perma.cc/9WZ2-J9Y9 (dark archive)]; Jane Mayer, *How Russia Helped Swing the Election for Trump*, NEW YORKER (Sept. 24, 2018), https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump [https://perma.cc/49J3-TDEN (dark archive)].

infrastructure.[425] In response, Congress appropriated money to improve the security of election technology,[426] and several government agencies began coordinating with the private sector on protection measures.[427]

Open source should already be treated as critical infrastructure as a part of the Information Technology sector and its maintenance a part of the National Critical Function of supply chain maintenance. However, in practice, the open-source community rarely interacts with the government, whether for emergency response planning or incident response coordination. The status quo is unsurprising. Open source's importance to society has been largely obscured given the nature of the technology and its community. Without a dedicated effort classifying open source as a critical infrastructure subsector in the Information Technology sector, open source's voice will remain unheard, and its needs will remain unmet.

The greatest weakness in critical infrastructure regulation today, which the Biden administration readily acknowledges, is that it is intentionally hands-off.[428] As elaborated above, the government offers incentives for private sector participation, but critical infrastructure designation, on its own, confers no power on the government to enforce the minimum-security standards or mandate information sharing by the private sector.

[425] *Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector*, U.S. DEP'T HOMELAND SEC. (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical [https://perma.cc/TKM5-V2EK].

[426] *See* Dustin Volz, *U.S. Spending Bill To Provide $380 Million for Election Cyber Security*, REUTERS (Mar. 21, 2018, 1:30 PM), https://www.reuters.com/article/us-usa-fiscal-congress-cyber/u-s-spending-bill-to-provide-380-million-for-election-cyber-security-idUSKBN1GX2LC [https://perma.cc/A95G-96AL].

[427] *See* Ellen Nakashima & Craig Timberg, *U.S. Agencies Mount Major Effort To Prevent Russian Interference in the Election Even Though Trump Downplays Threat*, WASH. POST (Oct. 21, 2020, 1:34 PM), https://www.washingtonpost.com/national-security/us-defends-russian-election-interference/2020/10/21/533b508a-130a-11eb-bc10-40b25382f1be_story.html [https://perma.cc/SCT3-RB7R (dark archive)].

[428] Presidential Decision Directive NSC-63 ("PDD-63") stated that "we should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector." THE WHITE HOUSE, PRESIDENTIAL DECISION DIRECTIVE/NSC-63, at 3 (1998), https://irp.fas.org/offdocs/pdd/pdd-63.pdf [https://perma.cc/XT83-DZX8]; *see, e.g.*, Howard A. Schmidt, *The Administration Unveils Its Cybersecurity Legislative Proposal*, WHITE HOUSE (May 12, 2011, 2:00 PM), https://obamawhitehouse.archives.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal [https://perma.cc/RTA5-XQFY] (describing how a proposal for mandatory security standards failed to pass).

2. Additional Roles for Government To Secure Open Source

Designating open source as critical infrastructure is not sufficient on its own.[429] There are various other roles the government can play, each with their own regulatory tools, to enhance efforts to secure critical infrastructure. The most successful options are those that coerce market behavior rather than rely on voluntary participation. Google itself has called on the government "to take a more proactive role in identifying and protecting open-source projects that are critical to internet security."[430]

a. Government as a Coordinator

Government can address open source's coordination problem by coercing private sector entities who would not otherwise participate—Irresponsible Consumers—to come to the table and ensuring the open-source community is invited as well. When applied, this model has proven effective at averting the mass exploitation of critical vulnerabilities like Log4Shell.[431]

i. Information Gathering

The first step in securing critical infrastructure must be gaining a complete and accurate understanding of the open-source ecosystem. There is no map of the open-source ecosystem in terms of which projects are used where the way

[429] *See* Ellen Nakashima & Tim Starks, *U.S. National Cyber Strategy To Stress Biden Push on Regulation*, WASH. POST (Jan. 5, 2023, 6:00 PM), https://www.washingtonpost.com/national-security/2023/01/05/biden-cyber-strategy-hacking/ [https://perma.cc/P2N7-LV5C (dark archive)]; Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 ("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.").

[430] Igor Bonifacic, *Google Wants To Work with Government To Secure Open-Source Software*, ENGADGET (Jan. 13, 2022, 3:48 PM), https://www.engadget.com/google-open-source-private-public-partnership-204840652.html [https://perma.cc/PWR3-GF57] ("In a blog post the company published following the White House's Log4j vulnerability summit on Thursday, Kent Walker, president of global affairs and chief legal officer at Google and Alphabet, said the country needs a public-private partnership that will work to properly fund and staff the most essential open-source projects.").

[431] Chester Wisniewski, *Log4Shell: No Mass Abuse, but No Respire, What Happened?*, SOPHOS NEWS (Jan. 24, 2022), https://news.sophos.com/en-us/2022/01/24/log4shell-no-mass-abuse-but-no-respite-what-happened/?cmp=30726 [https://perma.cc/SF27-7XFL] ("Sophos believes that the immediate threat of attackers mass exploiting Log4Shell was averted because the severity of the bug united the digital and security communities and galvanised people into action. This was seen back in 2000 with the Y2K bug and it seems to have made a significant difference here. As soon as details of the Log4Shell bug became clear, the world's biggest and most important cloud services, software packages and enterprises took action to steer away from the iceberg, supported by shared threat intelligence and practical guidance from the security community.").

there is for other critical infrastructure, such as telecommunications services[432] and nuclear reactors.[433] Without these maps, the government cannot identify where projects are vulnerable and which projects are overused. This knowledge informs policy; the government designs subsidy programs to bridge the digital divide[434] and support a failing nuclear industry.[435] And the government is uniquely positioned to see the forest for the trees.[436]

The government can obtain information from the private sector in a variety of ways. For instance, it can impose mandate reporting requirements, such as requiring Section 9 entities to report the open-source projects they rely on by providing the government with comprehensive SBOMs.[437] The government is already planning to collect SBOMs for federal systems in a central database; including private sector SBOMs that would enhance insight into the ecosystem.[438] The financial sector is already considering similar mandatory disclosure requirements on cybersecurity risk management, strategy, and governance policies.[439] These requirements can be expanded to include inventory reports as well.

[432] *Maps*, FED COMMC'NS COMM'N, https://www.fcc.gov/reports-research/maps/ [https://perma.cc/365N-SVFG].

[433] *Map of Power Reactor Sites*, U.S. NUCLEAR REGUL. COMM'N (July 17, 2020), https://www.nrc.gov/reactors/operating/map-power-reactors.html [https://perma.cc/58NT-5782].

[434] *See Auction 904: Rural Digital Opportunity Fund*, FED COMMC'NS COMM'N, https://www.fcc.gov/auction/904 [https://perma.cc/DYP3-KWK6] (describing the FCC's efforts to increase home internet connectivity through the Rural Digital Opportunity Fund).

[435] *See* MARK HOLT & PHILLIP BROWN, CONG. RSCH. SERV., REP. NO. 46820, U.S. NUCLEAR PLANT SHUTDOWNS, STATE INTERVENTIONS, AND POLICY CONCERNS 1 (2022), https://crsreports.congress.gov/product/pdf/R/R46820/3 [https://perma.cc/8UNB-BSYB (staff-uploaded archive)] (noting that although "[t]he United States has the largest nuclear power plant fleet in the world," its "nuclear power industry in recent years has been facing economic and financial challenges").

[436] *See* Geller, *Lesson from Log4j*, *supra* note 121 (quoting open-source SBOM advocate and CISA senior adviser Allan Friedman saying that the government has "a very global view of software" and "can help prioritize what are the projects that are critical to the national mission and also where we may not have enough existing resources").

[437] The government already has imposed mandatory reporting requirements for certain cyber incidents. *See generally* Cyber Incident Reporting for Critical Infrastructure Act, Pub. L. No. 117-103, § 103, 136 Stat. 1038, 1042–44 (2022) (codified at 6 U.S.C. § 681b (2022)) (providing an example of such requirements).

[438] *See* Exec. Order No. 14,028, 86 Fed. Reg. 26633, 26637–38 (May 12, 2021).

[439] U.S. SEC. & EXCH. COMM'N, FACT SHEET: PUBLIC COMPANY CYBERSECURITY; PROPOSED RULES 2, https://www.sec.gov/files/33-11038-fact-sheet.pdf [https://perma.cc/5P34-UV92] ("In addition to incident reporting, the SEC proposed to require enhanced and standardized disclosure on registrants' cybersecurity risk management, strategy, and governance.").

Alternatively, Congress can leverage existing DHS authorities and direct the agency to identify the most critical open-source projects.[440] The executive and legislative branches have already placed DHS at the center of cyber incident reporting.[441] But, given the shortcomings of DHS's critical asset identification process, Congress may instead opt to direct the Census to use its resources to collect information about open-source's uses in the private sector. The Census already "produces [reports of] economic data across the entire economy on a monthly, quarterly, yearly, and five-year basis,"[442] one of which already focuses on inventory data[443] and another which can be used to measure corporate contribution to open-source software.[444] Unlike participation with DHS information gathering efforts, responding to the Census is mandated under law.[445]

The open-source community has already made headway on this front, but its efforts were limited by resources and access to the private sector users of open source.[446] Government support for information gathering can augment the private sector's efforts to do the same. But to do so, its interventions must achieve meaningful cooperation from the private sector.

[440] For example, Provisions of the 2017 National Defense Authorization Act related to national preparedness against electromagnetic threats and hazards required DHS to determine, to the extent practicable, "the critical utilities and national security assets and infrastructure that are at risk." National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 1913(a)(3), 130 Stat. 2685–86 (codified at 6 U.S.C. § 195(f) (2016)); *see also* Exec. Order No. 13,865, 84 Fed. Reg. 12041, 12044 (Mar. 26, 2019) ("Within 90 days of the date of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs and other agencies as appropriate, shall identify and list the national critical functions and associated priority critical infrastructure systems, networks, and assets, including space-based assets that, if disrupted, could reasonably result in catastrophic national or regional effects on public health or safety, economic security, or national security.").

[441] *See* Eric Geller, *Biden Appointees Split on Key Cyber Bill*, POLITICO (Mar. 7, 2022, 4:30 AM), https://www.politico.com/news/2022/03/07/biden-appointees-split-key-cyber-bill-00014368 [https://perma.cc/ABG4-K57R] (discussing the DHS support of controversial cybersecurity bill).

[442] *Business and Economy*, U.S. CENSUS BUREAU (Oct. 5, 2022), https://www.census.gov/topics/business-economy.html [https://perma.cc/SB4P-TPWN].

[443] *Manufacturing and Trade Inventories and Sales, October 2022*, U.S. CENSUS BUREAU (Dec. 15, 2022), https://www.census.gov/mtis/www/data/pdf/mtis_current.pdf [https://perma.cc/2SJN-NPT3].

[444] *See* Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 (discussing how a U.S. Census Bureau survey could be improved to improve open-source software).

[445] *See* 13 U.S.C. § 221(a).

[446] *See* FRANK NAGLE, JESSICA WILKERSON, JAMES DANA & JENNIFER L. HOFFMAN, THE LINUX FOUND., CORE INFRASTRUCTURE INITIATIVE & THE LAB. FOR INNOVATION SCI. AT HARV., VULNERABILITIES IN THE CORE: PRELIMINARY REPORT AND CENSUS II OF OPEN SOURCE SOFTWARE 6–7, https://www.coreinfrastructure.org/wp-content/uploads/sites/6/2020/02/census_ii_vulnerabilities_in_the_core.pdf [https://perma.cc/W88K-WNJ5].

ii. Resource Allocation

Government, equipped with insight into the open-source ecosystem, can foster public-private collaborations to ensure security efforts and resources are being directed to the highest priority projects. Corporate beneficiaries of open-source software are a largely untapped resource. Many Contributing Consumers, such as Google and IBM, not only donate funds, but they also have full-time developers whose sole responsibility is to contribute to open-source projects.[447] This should be standard practice.

The private sector fails to invest sufficient resources into open-source security because of irrational preferences. As discussed earlier, the notion that security investments are not in a company's best interests is driven by the tragedy of the commons problem. The government can help change irrational preferences by solving the problems that give rise to these incorrect premises.[448] Large groups exacerbate the free-rider problem, but with forced coordination, a large group can incentivize contributions because the burden on any one entity is reduced.[449] Moreover, with the government playing the role of coordinator, open-source investment becomes a repeat game; when parties are forced to coordinate on an ongoing basis, they can no longer get away with free-riding.[450] Further, by forcing coordination, the government has the opportunity to correct the pervasive belief that open source is well-funded, encouraging more contribution.[451]

[447] *See, e.g.*, Sophia Vargas, *Open Source by the Numbers at Google*, GOOGLE OPEN SOURCE BLOG (Aug. 5, 2020), https://opensource.googleblog.com/2020/08/open-source-by-numbers-at-google.html [https://perma.cc/FYP5-MHXL] ("[M]ore than 9% of Alphabet's full time employees actively contributed to public repositories on git-on-borg and GitHub."); *see also* Daniel Oberhaus, *The Internet Was Built on the Free Labor of Open Source Developers. Is That Sustainable?*, VICE (Feb. 14, 2019, 9:30 AM), https://www.vice.com/en/article/43zak3/the-internet-was-built-on-the-free-labor-of-open-source-developers-is-that-sustainable [https://perma.cc/2TS9-8GKS] (discussing IBM's involvement in contributing to open-source projects from the mid-1990s).

[448] *See generally* Anomaly, *supra* note 266 (discussing the concept of "public goods" and the role governments play in providing them).

[449] While a large group can exacerbate a free-rider problem, with forced coordination between parties, a large group can have a positive effect on contributions despite the fact that it dilutes the effect of marginal returns. R. Mark Isaac, James M. Walker & Arlington W. Williams, *Group Size and the Voluntary Provision of Public Goods*, 54 J. PUB. ECON. 1, 4–5 (1994).

[450] *See generally* MICHAEL TAYLOR, ANARCHY AND COOPERATION (1976) (discussing the government's role in providing public goods).

[451] *See* EGHBAL, *supra* note 116, at 107 ("The pervasive belief, even among stakeholders such as software companies, that open source is well-funded, makes it harder to generate support. Some infrastructure projects operate sustainably, either because they have a working business model or sponsorship, or because their required upkeep is limited. An unfamiliar audience will also associate open source with enterprise companies like Red Hat or Docker and assume the problem has been solved. However, these situations are the outliers, not the rule.").

Resource allocation efforts need not rely on the market to identify the projects that need to be resourced. The open-source community has already used corporate funding to make progress on that front; with more private sector investment, it can do a lot more. OpenSSF's Alpha-Omega project aims to "work with the maintainers of the most critical open source projects to help them identify and fix security vulnerabilities and improve their security posture" and "identify at least 10,000 widely deployed," though not as critical, "projects where it can apply automated security analysis, scoring, and remediation guidance to their open-source maintainer communities."[452]

iii. Information Sharing

The government has many bodies at its disposal that can aid with coordinated information sharing between the public sector, the private sector, and the open-source community, particularly with critical infrastructure regulation. CISA, DHS, and the Commodity Futures Trading Commission, as well as the Federal Trade Commission, Treasury, and military, are but a few of the bodies that could coordinate. Beyond that, the government could rely on established disclosure systems to disclose information from the private sector to the public.[453]

Open source's inclusion in these government-coordinated information sharing bodies can provide it with intelligence that is currently only made available to private sector entities. Critical sectors are supported by Sector Risk Management Agencies—federal agencies specifically tasked with overseeing and reinforcing security within those sectors.[454] Critical infrastructure entities can opt to join Sector Coordinating Councils ("SCCs"), which are self-organized and self-governed bodies made up of private sector trade organizations and individual critical infrastructure owners and operators.[455] SCCs may also support independently organized Information Sharing and Analysis Centers ("ISACs") specific to their sector to facilitate information sharing among stakeholders. The National Council of ISACs currently lists twenty-seven member organizations.[456] The federal government is leveraging the WaterISAC specifically to provide water utilities with the expertise, threat

[452] *Alpha-Omega*, OPENSSF, https://openssf.org/community/alpha-omega/ [https://perma.cc/KJC9-7BDY].

[453] Securities Regulation is one example of where the government does rely on a disclosure system. *See, e.g.*, Act of July 29, 1968, Pub. L. No. 90-439, 82 Stat. 454 (codified as amended at 15 U.S.C. §§ 78m(d)-(e), 78n(d)-(f) (2015)) (enacting disclosure requirements for corporate take-overs).

[454] *See* CISA, NATIONAL CRITICAL FUNCTIONS, *supra* note 422, at 1.

[455] DEP'T OF HOMELAND SEC., CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL CHARTER 3 (2020), https://www.cisa.gov/sites/default/files/publications/cipac-charter-november-30-2020-508.pdf [https://perma.cc/SJK9-NHBR].

[456] NAT'L COUNCIL ISACS, https://www.nationalisacs.org/ [https://perma.cc/U6S2-G5JU].

information, and resources needed to secure their networks.[457] Open source should be able to join, and would benefit significantly from, a private, nonprofit ISAC that supports the information technology sector, where it can learn business information related to threat vectors and vulnerabilities that would otherwise be confidential.[458]

Open source can also benefit from information sharing by the government itself. Being identified as a Section 9 entity grants access to the National Risk Management Center ("NRMC"), which endeavors to "identify, analyze, prioritize, and manage the most significant risks to the Nation's critical infrastructure."[459] Participation in the NRMC benefits the open-source community by granting it access to federal classified information about threats that could impact their projects, among other things.

These government efforts to coordinate information sharing fall short because their access to information is limited. Although the government encourages the private sector to report cyber incidents, the private sector could opt not to. After the Colonial Pipeline attack, in which a "relatively unsophisticated" ransomware attack shut down America's largest refined products pipeline for several days, then-director of CISA, Brandon Wales, noted that he did not think Colonial would have notified CISA about the attack unless the Federal Bureau of Investigation had prompted them to.[460] The value of government information sharing is only as good as the information it has to share. This underlines the importance of reforming its information gathering efforts to address the private sector's lack of participation.

The government also maintains several vulnerability databases that foster information sharing. These databases are incomplete, however, because members of the private sector fail to report vulnerabilities they discover for fear

[457] *See* Starks, *U.K. Attack*, *supra* note 320 ("'What keeps me up at night are those smaller systems that don't have the cybersecurity staff or don't have the controls,' the director of infrastructure cyber defense at the Water Information Sharing and Analysis Center (WaterISAC), Jennifer Lyn Walker, told me.").

[458] *Id.*

[459] CISA, NATIONAL CRITICAL FUNCTIONS, *supra* note 422, at 2. Today, the National Risk Management Center at CISA has adopted an "evolved approach" to critical infrastructure risk management, which relies heavily on public-private collaborations to conduct cross-sector analyses and developing functionality-specific approaches to the identification, prioritization, and protection of critical infrastructure. *See id.*; *see also National Risk Management*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.dhs.gov/cisa/national-risk-management [https://perma.cc/3GQB-56WR].

[460] Clare Duffy, *Colonial Pipeline Attack: A 'Wake Up Call' About the Threat of Ransomware*, CNN (May 16, 2021, 8:35 AM), https://www.cnn.com/2021/05/16/tech/colonial-ransomware-darkside-what-to-know/index.html [https://perma.cc/NN7L-29HA]; Samantha Schwartz, *CISA Left in the Dark During Colonial Pipeline's Initial Response*, CYBERSECURITYDIVE (May 12, 2021), https://www.cybersecuritydive.com/news/colonial-pipeline-ransomware-cisa-senate-hearing/600029/ [https://perma.cc/WAN8-9AYG] (noting former Director Brandon Wale's comments).

of public retribution or legal liability.[461] Currently, there are no liability protections for vulnerability disclosure. These databases are also limited by security researchers' hesitation to disclose.[462] After Heartbleed, there was significant turmoil around the suspicion that the National Security Agency had known about the vulnerability and, rather than disclose it, had opted to stockpile for future exploitation.[463] While the Obama administration denied any prior knowledge of the vulnerability, it confirmed that in certain circumstances, the national security interest of keeping a vulnerability secret outweighs the public benefits of disclosing it.[464] Encouraging the open-source community and the private sector will require assuaging their respective fears and clearing up misinformation.

Finally, the government can dispel misconceptions within its own ranks to better protect the open-source community. In 2013, the Internal Revenue Service ("IRS") targeted the open-source community for investigation, suspicious of its qualifications for tax-exempt status.[465] For example, the Django Software Foundation cannot fund the Django project it supports without risk of losing its 501(c)(3) status.[466] The root of the IRS's consternation: that commercial entities could use the software.[467] The open-source community struggles to maintain 501(c)(3) status to this day.[468] Without reform, every

[461] *See* Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb & Lei Zhou, *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*, 11 J. COMPUT. SEC. 431, 444–45 (2003) (describing negative stock price reactions when vulnerabilities are disclosed).

[462] *See, e.g.*, Bradley Barth, *Row over Data Leak Disclosure by Journalist Further Erodes Research Trust in Government*, SC MEDIA (Oct. 15, 2021), https://www.scmagazine.com/analysis/bug-bounties/row-over-data-leak-disclosure-by-journalist-further-erodes-researchers-government-trust [https://perma.cc/SUW9-YRUA].

[463] Kim Zetter, *Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA*, WIRED (Apr. 15, 2014, 6:30 AM), https://www.wired.com/2014/04/obama-zero-day/ [https://perma.cc/F7EC-LQWK].

[464] Michael Daniel, *Heartbleed: Understanding when We Disclose Cyber Vulnerabilities*, WHITE HOUSE (Apr. 28, 2014, 3:00 PM), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities [https://perma.cc/5DT3-5DN3].

[465] EGHBAL, *supra* note 116, at 110–11 ("In 2013, a controversy revealed that the IRS had internally identified a list of groups applying for tax-exempt status that would require further scrutiny; 'open source' was one of these.").

[466] *Id.* at 111.

[467] Jim Nelson, *The New 501(C)(3) and the Future of Free Software in the United States*, JIM NELSON + YORBA FOUND. ARCHIVES (June 30, 2014), https://blogs.gnome.org/jnelson/2014/06/30/the-new-501c3-and-the-future-of-free-software-in-the-united-states/ [https://perma.cc/79ZY-3REZ].

[468] Karl Mill, *More 501(C)(3) Rejections: Open Source Software Edition*, MILL L. CTR. (July 26, 2022), https://www.mill.law/blog/more-501c3-rejections-open-source-software-edition [https://perma.cc/WB6H-QJYB].

dollar successfully invested by the private sector into open source threatens to disqualify it for future support.

b. Government as a Standards Body

The government regularly recommends industry best practices to ensure public security and safety. At times, these standards are mandatory. For example, Congress specifically authorized DHS to conduct inspections and enforce regulatory standards against chemical manufacturing facilities that pose a high risk for malicious exploitation.[469] So far, however, there are no mandatory minimum standards for the software industry, related to open source or not. Indeed, the government generally prefers letting industry develop its own standards, "[e]ven in circumstances where there is heightened urgency to meet" critical public interest needs.[470]

In some sectors, the government addresses a market failure by encouraging the industry to establish minimum standards independently. This is most effective when paired with the threat of regulation should the industry fail to address the issue. For example, the government urged the healthcare sector to develop open standards for information sharing because the lack of interoperability between private sector databases was impeding the government's ability to deliver healthcare to the public.[471] Ultimately, the government was forced to implement a rule mandating interoperability for data

[469] *See* FRANK GOTTRON, CONG. RSCH. SERV., REP. NO. IF10853, CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (2020), https://crsreports.congress.gov/product/pdf/IF/IF10853/6 [https://perma.cc/R57J-RZJ9 (staff-uploaded)] (noting that Chemical Facility Anti-Terrorism Standards were first authorized by Congress in 2007).

[470] Stacy Baird, *The Government at the Standards Bazaar*, 18 STAN. L. & POL'Y REV. 35, 72 (2007) (collecting examples of consortia-developed standards). There are many examples of consortia-developed standards—for an extensive list, see *id.* at 42–44.

[471] *See* MARKLE FOUND., THE DATA STANDARDS WORKING GROUP REPORT AND RECOMMENDATIONS 21, 51–57 (2003), https://markle.org/app/uploads/2022/03/healthreport.pdf [https://perma.cc/3J75-8HAS]. *See generally* MARKLE FOUND. & THE ROBERT WOOD JOHNSON FOUND., ACHIEVING ELECTRONIC CONNECTIVITY IN HEALTHCARE: A ROADMAP FROM THE NATION'S PUBLIC AND PRIVATE-SECTOR HEALTHCARE LEADERS (2004), https://markle.org/app/uploads/2022/03/roadmap_11_15.pdf [https://perma.cc/8GFE-3BYX] (recommending strategies for better organization of the U.S. healthcare industry); U.S. GOV. ACCOUNTABILITY OFF., REP. NO. IMTEC-93-17, AUTOMATED MEDICAL RECORDS: LEADERSHIP NEEDED TO EXPEDITE STANDARDS DEVELOPMENT (1993), http://archive.gao.gov/t2pbat5/149267.pdf [https://perma.cc/N8JC-A35Q] (discussing standards for medical records to improve medical record-keeping); U.S. GOV. ACCOUNTABILITY OFF., REP. NO. IMTEC-91-5, MEDICAL ADP SYSTEMS: AUTOMATED MEDICAL RECORDS HOLD PROMISE TO IMPROVE PATIENT CARE (photo. reprt.) (1991), http://archive.gao.gov/t2pbat8/143217.pdf [https://perma.cc/P5ST-ZFDR] (reporting on the benefits and drawbacks of automating patient records in healthcare).

exchange and developed a roadmap for its implementation.[472] The government can adopt a similar approach with open source: encouraging the private sector to collaborate with the open-source community on security standards and stepping in should these voluntary efforts fail.

However, standards setting organizations rely on market incentives, and the narrative that it is in a company's best interest to coordinate with competitors.[473] Open source, like environmental protection, lacks the market incentives to drive this behavior; Irresponsible Consumers are unlikely to come to the negotiation table.[474] In the environmental space, Congress responded to the market's "failure to foresee and control the untoward consequences of modern technology" with mandatory standards.[475] The Biden administration's national cyber strategy emphasizes the same need in the software security space.[476]

c. Government as a Consumer

The government can expand on its current efforts to shape the software market through its power as a consumer with a targeted focus on open source. The federal government's budget for civilian agencies' information technology needs is estimated to be sixty-five billion dollars in 2023, not including the technology-heavy military and intelligence agencies.[477] The federal government represents a significant portion of the market for information technology products and services; to preserve this customer base, companies are willing to acquiesce to its requests.

The government already flexes its dominance as a consumer to improve the security of its information technology. To address the rise in cyberattacks and the lax security practices of its vendors, the government has mandated a

[472] *See Policies and Technology for Interoperability and Burden Reduction*, CMS.GOV, https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index [https://perma.cc/4YKL-T44E]; Advancing Interoperability and Improving Prior Authorization Processes, 87 Fed. Reg. 76238, 76238 (proposed Dec. 13, 2022) (to be codified in scattered sections of 42 C.F.R.).

[473] Baird, *supra* note 470, at 36, 56–57.

[474] *See* Mark Sagoff, *The Economy of the Earth*, *in* LAW AND THE ENVIRONMENT: A MULTIDISCIPLINARY READER 49 (Robert V. Percival & Dorothy C. Alevizatos eds., 1997) (summarizing the economic perspective on environmental problems); Daniel C. Esty, *Toward Optimal Environmental Governance*, 74 N.Y.U. L. REV. 1495, 1503–08 (1999) (describing market failures as an underlying cause of environmental harms).

[475] Lee, *Environmental Economics*, *supra* note 285, at 481 (quoting H.R. Rep. No. 91-378, at 3 (1969), reprinted in 1969 U.S.C.C.A.N. 2751, 2753).

[476] *See* Nakashima & Starks, *supra* note 429.

[477] *Information Technology and Cybersecurity Funding*, *in* ANALYTICAL PERSPECTIVES, BUDGET OF THE UNITED STATES GOVERNMENT FISCAL YEAR 2023, at 233, 233 (2023), https://www.govinfo.gov/content/pkg/BUDGET-2023-PER/pdf/BUDGET-2023-PER-6-3.pdf [https://perma.cc/JMN3-TGEN].

series of new requirements that contractors must comply with to continue selling to the government. Some contracting regulations impose certification requirements, such as "Common Criteria testing"[478] and FedRAMP, which requires federal cloud service providers obtain certification that they are complying with minimum security standards before selling to the government.[479] The government can expand on the recent software security requirements imposed in the EO and require entities building critical infrastructure software to get certified ensuring the open-source projects they are using are well-maintained and that their internal security practices are consistent with industry best practices.

d. *Government as a Supplier*

In addition to coercing the private sector to play a bigger role in securing open source, the government can itself fill some of the gaps in resources and security practices.[480] Experts in the open-source community say that many of the tools and techniques needed to secure open source already exist; they just need funding to scale up.[481]

i. Resource Donor

Government donations can supply resources directly and encourage third-party donations indirectly. Congress can appropriate funding specifically for open-source community support. Economics tells us the government plays an important role in subsidizing producers of public goods when the market fails to provide sufficient supply.[482] For example, the government already subsidizes the protection of election infrastructure and the delivery of broadband services

[478] Nancy Mead, *The Common Criteria*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (2013), https://www.cisa.gov/uscert/bsi/articles/best-practices/requirements-engineering/the-common-criteria [https://perma.cc/4H96-A29U].

[479] *Program Basics*, FED. RISK & AUTHORIZATION MGMT. PROGRAM, https://www.fedramp.gov/program-basics/ [https://perma.cc/Z6AF-87KR].

[480] *See* Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 ("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.").

[481] *See* Pattison-Gordon, *supra* note 77.

[482] *See* CORNES & SANDLER, *supra* note 99, at 50–58 (describing the economic theory behind externalities and how they interact with public goods); *see also* STIGLITZ, WHITHER SOCIALISM?, *supra* note 262, at 7 (stating that government's role is "to correct the well-defined market failures," "to provide public goods and to levy taxes to finance them," and "to take actions to ensure that markets are actually competitive").

in rural areas.[483] OpenSSF told the White House that it needed $147.9 million to maximize the impact of its workstreams and develop a strategy for long-term open-source security—this is less than half the amount of money that Congress allocated to secure election infrastructure.[484]

Beyond the obvious benefit of immediate resources where resources are needed, studies show when first-movers visibly make large contributions, others are more likely to follow suit.[485] An empirical study found that government contribution specifically to open source actually encourages more firm contributions, not less.[486] To enhance this effect, the government can offer tax credits to individuals and companies who surpass a certain threshold of open-source contributions.[487]

Once collected, resources can be funneled to existing open-source support organizations. These organizations have diverse funding models, sector-expertise, channels to distribute funds, and strong relationships with the open-source community.[488] In addition to OpenSSF, Open Technology Fund ("OTF") and OSTIF are strong contenders. OTF was established specifically to fund open-source projects that benefit society; while its original focus was on social-justice oriented projects, it is beginning to dedicate more efforts to project security and long-term maintenance.[489] As a security services provider,

[483] *See Election Security Funds*, U.S. ELECTION ASSISTANCE COMM'N, https://www.eac.gov/payments-and-grants/election-security-funds [https://perma.cc/LAE2-55GA]; *see also Auction 904: Rural Digital Opportunity Fund*, *supra* note 434.

[484] *See supra* note 352 and accompanying text.

[485] Jen Shang & Rachel Croson, *A Field Experiment in Charitable Contribution: The Impact of Social Information on the Voluntary Provision of Public Goods*, 119 ECON. J. 1422, 1434–36 (2009). *See generally* Rainald Borck, Björn Frank & Julio R. Robledo, *An Empirical Analysis of Voluntary Payments for Information Goods on the Internet*, 18 INFO. ECON. & POL'Y 229 (2006) (presenting results from field study on voluntary contributions for an information public good provided through the internet).

[486] Reisinger et al., *supra* note 102, at 489.

[487] "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." Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 (proposing a tax credit for direct expenses related to open-source development, such as cloud computing resources, and uncompensated time spent developing open-source resources).

[488] *See* Frederic Lardinois, *The OpenInfra Foundation Launches 'Directed Funding' as a New Way To Support Open Source Projects*, TECHCRUNCH (June 7, 2022, 7:00 AM), https://techcrunch.com/2022/06/07/the-openinfra-foundation-launches-directed-funding-as-a-new-way-to-fund-open-source-projects/ [https://perma.cc/563P-FBL6]. *Compare* TIDELIFT, https://tidelift.com/ [https://perma.cc/VE7D-NE6E] (describing a subscription model through which companies contribute funds that go to projects that agree in advance to meet minimum standards imposed by Tidelift), *with* OPEN SOURCE COLLECTIVE, https://www.oscollective.org/ [https://perma.cc/G2TG-CQ9D] (describing a model distributing donations to open source projects at the nonprofit's discretion).

[489] OPEN TECH. FUND, https://www.opentech.fund/ [https://perma.cc/CY9Z-ZD6N].

OSTIF has the ability to identify projects that need its services and is proactively told by the community which projects need services.

The government can also attempt to fund open-source projects directly.[490] Supporting a critical project could involve grants as small as $50,000.[491] Without a complete picture of the open-source ecosystem, however, it cannot know which projects the checks should be addressed to. Instead, the government can avoid picking winners and losers by inviting eligible parties to apply with an explanation justifying their need. The National Science Foundation already makes some funding available to the open-source community through grants, but the funds often do not make it to the projects that need them the most because the projects were abandoned, the maintainer is unaware of the availability of funds, the maintainer is unaware of the need for funds, or the maintainer is unable to effectively apply for the funds.[492] Grant applications are notoriously arduous;[493] without expertise in grant applications and the willingness and time to dedicate to the effort, that money is unattainable despite being theoretically available.

Rather than impose the burden of grant applications on project maintainers, the government can invite federal agencies and private companies to apply for grants on behalf of the open-source projects most important to them. This returns to the paramount importance of forcing the open-source ecosystem to coordinate to identify the most important projects to any given critical infrastructure sector.

[490] Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 ("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.").

[491] Geller, *Lesson from Log4j*, *supra* note 121 (quoting the head of OpenSSF describing the simplicity of core critical software and stating that grants of $50,000 or $80,000 could make a "substantial" difference).

[492] *Pathways To Enable Open-Source Ecosystems (POSE)*, NAT'L SCI. FOUND., https://www.nsf.gov/pubs/2022/nsf22572/nsf22572.htm [https://perma.cc/497Z-3XCX].

> The NSF is specifically funding new OSE managing organizations. Each organization will create and maintain the infrastructure for a specific OS product or class of products. They want "more secure open source products, increased coordination of developer contributions, and a more focused route to impactful technologies." Best of all, the NSF is putting its money where its mouth is. They anticipate giving out 30 awards: 20 Phase I awards of up to US$ 300,000 each for one year and 10 Phase II awards of up to US$ 1,500,000 for up to two years.

Joshua Pearce, *The National Science Foundation Bets Big on Open Source*, OPENSOURCE.COM (Mar. 6, 2022), https://opensource.com/article/22/3/national-science-foundation-open-source [https://perma.cc/3SHQ-EHF4] (citation omitted).

[493] EGHBAL, *supra* note 116, at 108 ("If I wanted to get a grant, I wouldn't even know where to start." (quoting Kyle Kemp, freelance developer and open source contributor)).

ii. Open-Source Contributor

The government can also lead by example and contribute to the open-source community in the form of developer support. In 2016, the Obama administration released a Federal Source Code policy that required, among other things, that custom projects built by or for the government open-source at least twenty percent of their codebases.[494] Unfortunately, studies of the pilot program found it neither increased the rate at which federal open-source projects were created nor the rate at which the public used those projects.[495] That is not to suggest the government is not a valuable contributor to open-source software. One of the most significant contributions to the Linux kernel in history was made by the National Security Agency.[496]

The government can also contribute to the open-source community by building useful open-source projects.[497] One prime example is in-toto, a tool built by a team of developers to secure software development.[498] It was not focused specifically on open source but grew out of the recognition of the systemic threat software vulnerabilities posed.[499] It is an open-source tool, free to use, and its developers believe that, if implemented, it could have prevented between 83% and 100% of thirty major supply chain attacks dating back to 2010.[500] A systematic review of its successes concludes that this government-

[494] Memorandum from Tony Scott & Anne E. Rung, Off. of Mgmt. & Budget, Exec. Off. of the President to the Heads of Dep'ts and Agencies 8 (Aug. 8, 2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf [https://perma.cc/MEC2-Q7LL]; *see also* Tony Scott, *The People's Code*, CIO.GOV (Aug. 11, 2016), https://www.cio.gov/2016/08/11/peoples-code.html [https://perma.cc/8DQC-RJNF]; Andrew Tarantola, *New Policy Demands 20 Percent of Federal Code Be Open Source*, ENGADGET (Aug. 9, 2016, 1:24 PM), https://www.engadget.com/2016-08-09-new-policy-demands-20-percent-of-federal-code-be-open-source.html [https://perma.cc/9RQB-CLHU]; CODE.GOV, https://code.gov/ [https://perma.cc/9Y74-42MV].

[495] JAKE RASHBASS & MAIRI ROBERTSON, HARV. KENNEDY SCH., THE PEOPLE'S CODE: AN ANALYSIS OF PUBLIC ENGAGEMENT WITH THE US FEDERAL GOVERNMENT'S OPEN SOURCE PILOT PROGRAM 5 (2019), https://ash.harvard.edu/files/ash/files/20190506_pae_final_ash.pdf [https://perma.cc/E8HY-KATF].

[496] *See* SMALLEY, *supra* note 106.

[497] For example, the U.S. Digital Service regularly develop and contribute to open-source tools that serve the public. *See, e.g.*, U.S. Digital Serv., *Tackling the Climate Crisis with Open Source*, MEDIUM (Apr. 27, 2022), https://medium.com/the-u-s-digital-service/tackling-the-climate-crisis-with-open-source-1db9b000a52a [https://perma.cc/VCG4-FPAJ].

[498] *See CI-ADDO-EN: Enhancing and Supporting a Community Testbed, Award Abstract #1205415*, NAT'L SCI. FOUND. (July 25, 2015), https://www.nsf.gov/awardsearch/showAward?AWD_ID=1205415 [https://perma.cc/UU8J-PPNM] (describing grant award for open-source program).

[499] Peter Elkind & Jack Gillum, *The U.S. Spent $2.2 Million on a Cybersecurity System That Wasn't Implemented—And Might Have Stopped a Major Hack*, PROPUBLICA (Feb. 2, 2021, 6:00 AM), https://www.propublica.org/article/solarwinds-cybersecurity-system [https://perma.cc/UJG9-2RRX].

[500] *Id.*

funded tool shows that "protecting the entirety of the [software] supply chain is possible."[501]

The government can continue similar efforts by allocating funding for researchers to develop open-source projects that can help secure the open-source community. However, these tools are ineffective unless widely adopted. In-toto has existed since 2016 and could have prevented the Solarwinds attack if it had actually been used.[502] Additionally, in-toto struggles to maintain the funding and developer-support it needs to meet growing demand. While the government may build a useful open-source tool, that tool, without dedicated attention, can fall prey to the same resource-limitations the rest of the open-source ecosystem struggles with. It can also gather dust unless its use is incentivized or mandated.

iii. Security-Services Provider

The government also supplies important security services to the public. CISA offers free risk assessments to critical infrastructure entities, services that are otherwise costly and time intensive.[503] It can supplement OSTIF's efforts by making its own cybersecurity teams available to the open-source community, increasing the likelihood that risk is identified and mitigated early in the supply chain.[504]

The government also provides critical infrastructure entities with free incident response coordination and support. The government advertises these services, welcoming companies to take advantage of them and, at times, seeking out entities proactively to offer these services. For example, within two days of being notified of the Solarwinds attack, the federal government activated a Cyber Unified Coordination Group with members from various relevant agencies and members of the private sector to coordinate a centralized

[501] Santiago Torres-Arias, Hammad Afzali, Trishank Karthik Kuppusamy, Reza Curtmola & Justin Cappos, *in-toto: Providing Farm-to-Table Guarantees for Bits and Bytes*, 28 USENIX SEC. SYMP. 1393, 1406–07 (2019).

[502] *See generally* Elkind & Gillum, *supra* note 499 (discussing how in-toto could have helped prevent the Solarwinds by blocking and revealing the attack proactively).

[503] *Shields Up*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/shields-up [https://perma.cc/AN8P-SB2X] ("Recognizing that many organizations find it challenging to identify resources for urgent security improvements, we've compiled free cybersecurity services and tools from government partners, and industry to assist.").

[504] *See* John Speed Meyers, Zack Newman & Jacobo McGuire, *The US Military Should Red-Team Open Source Code*, DEF. ONE (Aug. 10, 2022), https://www.defenseone.com/ideas/2022/08/military-should-red-team-open-source-code/375635/ [htt ps://perma.cc/XP5J-QV7J] (calling on the military to red-team, or test the security of, open-source software components on which it has become dependent and to share that information back to the open-source community).

response.[505] After the Log4Shell incident, CISA convened a call with the Joint Cyber Defense Collaborative to coordinate information sharing and response strategy between government and the private sector internationally.[506] Confusingly, the open-source community did not participate. As CISA explores how to expand use of the resulting model into additional critical infrastructure sectors, it should prioritize active inclusion of the open-source community in its work.[507]

The government can also expand its own vulnerability disclosure programs to gather threat information and crowdsource patches for open-source components. Each federal agency is currently required to develop and publish a vulnerability disclosure program.[508] These programs can be paired with bug bounty programs that offer cash to hackers for relevant vulnerability information and solutions.[509] The recent Hack DHS bug bounty program involved more than 450 vetted researchers identifying 122 vulnerabilities, 27 of which were critical.[510] The government was out of pocket no more than $125,600 for this valuable security information.[511] While the private sector conducts their own bug bounty programs, they often focus on open-source components they

[505] Vijay A. D'Souza, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response*, U.S. GOV'T ACCOUNTABILITY OFF. (Apr. 22, 2021), https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic [https://perma.cc/K8JE-S6BW].

[506] Justin Doubleday, *Officials Say Log4j Response Proves Out Promise of New Public*, FED. NEWS NETWORK (Feb. 9, 2022, 3:55 PM), https://federalnewsnetwork.com/cybersecurity/2022/02/officials-say-log4j-response-proves-out-promise-of-new-public-private-partnership/?readmore=1 [https://perma.cc/ZX3Y-F5KG] ("The agency used information from the JCDC and elsewhere to feed a Github repository of vulnerable products and associated patches. CISA also directed federal agencies to immediately patch Internet-connected devices containing Log4shell, while recommending private sector organizations do the same.").

[507] *See* Sara Friedman, *CISA Considers How To Integrate More Critical Infrastructure Sectors into JCDC Efforts*, INSIDE CYBERSECURITY (Apr. 4, 2022), https://insidecybersecurity.com/daily-news/cisa-considers-how-integrate-more-critical-infrastructure-sectors-jcdc-efforts [https://perma.cc/7XR6-528T (dark archive)] ("CISA is looking into how to expand the Joint Cyber Defense Collaborative model into additional critical infrastructure sectors working hand in hand with Sector Risk Management Agencies to drive down risk.").

[508] *Binding Operational Directive 20-01*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Sept. 2, 2020), https://www.cisa.gov/binding-operational-directive-20-01 [https://perma.cc/D6G3-4MAH].

[509] Studies have found bug bounty programs to be especially effective in the open-source context. Chujiao Ma, Matthew Bosack, Wendy Rothschell, Noopur Davis & Vaibhav Garg, *Wanted Hacked or Patched: Bug Bounties for Third Party Open-Source Software Components*, USENIX (Oct. 7, 2022), https://www.usenix.org/sites/default/files/opensourcebugbounty_login_final.pdf [https://perma.cc/6ZJB-W3Z5].

[510] Press Release, U.S. Dep't of Homeland Sec., "Hack DHS" Program Successfully Concludes First Bug Bounty Program (Apr. 22, 2022), https://www.dhs.gov/news/2022/04/22/hack-dhs-program-successfully-concludes-first-bug-bounty-program [https://perma.cc/F5PN-VGYP].

[511] *Id.*

independently maintain, rather than the source component they drew from, limiting the benefit the original maintainer derives.[512]

As a longer-term goal, the government should invest its security expertise and resources into supporting open-source education and training.[513] The government suffers the most from the cybersecurity workforce gap. And, if the Peters-Portman bill passes, CISA will be required to ramp up their hiring of open-source experts and agencies would be required to establish open-source program offices, which could spur the federal government's contribution to the open-source ecosystem.[514] Developing federal guidance on software security curricula and providing grants to schools offering it could help improve open-source literacy and train the next generation of security professionals.[515]

e. Government as an Enforcer

Government intervention can lean on incentives for compliance, but it is most effective when compliance is mandated. Sometimes, "coercively enforced government mandates (such as laws regulating pollution)" are "the only feasible way to achieve a goal that makes everyone better off."[516] With open source's tragedy of the commons problem, private actors are unlikely to act in the public's best interest without some amount of coercion.[517]

[512] *See, e.g.*, *Google Open Source Software Vulnerabilities Reward Program Rule*s, GOOGLE BUG HUNTERS, https://bughunters.google.com/about/rules/6521337925468160/google-open-source-software-vulnerability-reward-program-rules [https://perma.cc/S294-SNLC] ("Google's Open Source Software Vulnerability Reward Program recognizes the contributions of security researchers who invest their time and effort in helping us secure open source software released by Google (Google OSS). Through this program, we provide monetary rewards and public recognition to researchers who disclose vulnerabilities in Google OSS to us.").

[513] Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 ("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.").

[514] *See* Press Release, U.S. Senate Comm. on Homeland Sec. & Governmental Affs., Peters and Portman Introduce Bipartisan Legislation To Help Secure Open Source Software (Sept. 22, 2022), https://www.hsgac.senate.gov/media/majority-media/peters-and-portman-introduce-bipartisan-legislation-to-help-secure-open-source-software [https://perma.cc/TRU6-BDJY].

[515] Geller, *Lesson from Log4j*, *supra* note 121.

[516] Anomaly, *supra* note 266, at 110.

[517] *See* Nagle, *Strengthening Digital Infrastructure*, *supra* note 7 ("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

While DHS has limited authority to impose security requirements on critical infrastructure entities, Congress can step in to fill the gap. For example, Congress established the U.S. Nuclear Regulatory Commission ("NRC") to regulate civilian nuclear facilities.[518] The Commission imposed extensive safety and reporting requirements in response to evidence that the private sector would not on its own protect the public interest: the Three Mile Island nuclear reactor meltdown.[519]

Alternatively, federal agencies, including critical infrastructure sector risk management agencies, can take a more active role in securing critical infrastructure in the face of evidence that private sector efforts are insufficient. Following the largest blackout in U.S. history, a task force concluded the grid was vulnerable to malicious actors.[520] In response, the Federal Energy Regulatory Commission adopted mandatory and enforceable reliability standards with penalties for noncompliance.[521]

Mandatory security standards can go a long way towards securing open source in critical infrastructure.[522] The Cybersecurity Solarium Commission agrees: it suggested statutorily requiring a subset of Section 9 entities, the most

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.").

[518] *About NRC*, NUCLEAR REGUL. COMM'N (Aug. 10, 2022), https://www.nrc.gov/about-nrc.html [https://perma.cc/LN7W-HWN2].

[519] *See id.*; *Backgrounder on the Three Mile Island Accident*, NUCLEAR REGUL. COMM'N (Apr. 2022), https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html [https://perma.cc/H5A5-6CEU]; U.S. DEP'T OF HOMELAND SEC., NUCLEAR REACTORS, MATERIALS, AND WASTE SECTOR-SPECIFIC PLAN: AN ANNEX TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN 2–3 (2010), https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2010-508.pdf [https://perma.cc/MRJ6-YSBU]. *See generally* JOHN D. MOTEFF, CONG. RSCH. SERV., REP. NO. RL30153, CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION (2015), https://sgp.fas.org/crs/homesec/RL30153.pdf [https://perma.cc/QY7U-7K6F] (providing more examples of non-DHS federal regulation of critical infrastructure security).

[520] U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003, BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS 131–32 (2004), https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf [https://perma.cc/EVH6-PG5V] (discussing the source of the 2003 Northeast Blackout).

[521] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 17 Fed. Reg. 7368, 7370 (Feb. 7, 2008) (codified at 18 C.F.R. Part 40); *see FERC Approves New Reliability Standards for Cyber Security*, SEC. TODAY (Jan. 24, 2008), https://securitytoday.com/articles/2008/01/24/ferc-approves-new.aspx?admgarea=ht.government [https://perma.cc/A8AH-WXHN].

[522] *See* Herr et al., *supra* note 132 ("[A] clear legal-negligence standard for software vendors would improve security in the cyber ecosystem by incentivizing vendors to meet baseline security requirements for products and to provide more security support throughout product lifecycles. Clarifying liability would impose on final assemblers of software products—the entities responsible for placing a product in the consumer market, also called final goods assemblers—specific obligations for ensuring the security of all code incorporated in their final products, including open source packages.").

"systemically important," to participate in government-coordinated national risk identification and assessment efforts.[523] It also advised requiring these entities to adhere to a new "Security Certification" that would entail "common and sector-specific standards and expectations for the governance and execution of security operations."[524] The inaugural CSRB report on the Log4Shell incident echoed the Solarium's recommendations. It was especially concerned with the incentive structure around open-source software and stated that the government should consider software liability reform.[525] The Biden administration's national cyber plan broadly adopts the Solarium and CSRB calls for private sector software liability, though time will tell what the implementation of such a regime would look like.[526]

Mandatory security standards need not give rise to a flood of litigation. The Solarium report offered one way to mitigate this concern that would further the goal of boosting preventive measures: the statute could contain a safe harbor provision, shielding entities in "good-faith compliance" with security requirements from legal actions arising out of "instances when covered systems and assets are targeted, attacked, compromised, or disrupted through a cyberattack by a nation-state, designated transnational criminal group, or terrorist organization."[527] Alternatively or additionally, a liability shield could immunize companies and individuals from vulnerabilities arising out of libraries to which they otherwise diligently contributed. Whether the requirements are imposed on the largest companies above a revenue, profit, or user-base threshold, or on the ones that directly build software that supports National Critical Functions, a liability shield would encourage diligent adoption of required security measures.

Heightened cybersecurity standards on open-source components should not unfairly burden an already overwhelmed open-source community. Targeting open-source developers, who provide a public good for free, would chill contributions. Beyond harms to innovation and competition, this would compromise critical infrastructure security by further depleting the supply of open-source maintenance. The weight of these standards should fall only on the shoulders of those who commercially gain from using that public good. The European Union's Cyber Resiliency Act is an example of legislation intended to bolster the security of software and hardware *commercial products*. "In order

[523] *See* ANGUS KING & MIKE GALLAGHER, U.S. CYBERSPACE SOLARIUM COMM'N, MARCH 2020 REPORT 97–99 (2020), https://www.solarium.gov/report [https://perma.cc/3VBD-8JBV (staff-uploaded archive)] (click "Download Official Report").

[524] *Id.*

[525] CSRB LOG4J REPORT, *supra* note 138, at 28.

[526] *See* Nakashima & Starks, *supra* note 429.

[527] KING & GALLAGHER, *supra* note 523, at 98.

not to hamper innovation or research," the bill expressly excludes "open-source software [that is] developed or supplied outside the course of a commercial activity."[528]

Requirements must be designed carefully, to avoid overbroad impositions and underinclusive scope.[529] If done well, mandating coordination, information sharing, and minimum standards, these laws can prevent Irresponsible Consumers from free-riding unnoticed, can require their participation in attempts to map the open-source ecosystem, and can rectify the poor security practices that put critical infrastructure at risk. These ex-ante impositions can be enforced before an exploit occurs and it is too late. In the case of widespread, devastating impact, the government would have to intervene to secure the country and, as discussed above, remediation measures would be far costlier than upfront investment in preventative security. Further, given the nature of downed critical infrastructure, there is no remedy for the very real harm the public would suffer.

The government has long resisted calls to impose requirements on the commercial information technology industry, but it behooves it to consider imposing concrete security requirements now. In the case of open source, passive interventions will not be enough to secure critical infrastructure.

[528] Eur. Comm'n, Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020, at 15 (Sept. 15, 2022), https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act [https://perma.cc/4UAZ-ASCG] (click "Download") ("In order not to hamper innovation or research, free and open source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.").

[529] For example, it would be wise to avoid far-reaching prohibitions on anonymous or pseudonymous contributions, as Google once suggested. Depriving the open-source community of the ability to mask their identity undercuts a core feature of the culture and will discourage participation. Similarly, eradicating inactive repositories would be overbroad. For one, removing libraries risks breaking unknown programs that rely on them. Second, many projects remain stable without active contributions. Forcing developers to commit for the sake of committing would introduce more risk than it would solve. Simon Willison (@simonw), TWITTER (Aug. 4, 2022, 5:29 PM), https://twitter.com/simonw/status/1555304894919110657?s=20&t=V2ZWF8DHgOrOHqB3X0hKlg [https://perma.cc/4XTB-5F5J] (providing examples of projects that remain stable without recent commits and applauding GitLab, a project hosting platform, for reconsidering its brash decision to remove inactive projects from its servers entirely). Additionally, sweeping regulation to address all industries would be tactless. Security mandates should be tailored to each critical infrastructure sector's unique risk posture and technological capabilities. The FDA serves as a good example of an SMRA that worked closely with industry to design and update security regulations over time that address risks specific to the health sector while taking into account the industry's limitations.

Conclusion

The threat to open source increases with each passing day, and with it, the threat to our critical infrastructure.[530] As this Article demonstrates, without intervention, open-source resources will be depleted, rendering our most important systems vulnerable to attack. Today, Irresponsible Consumers parasitically profit from the resource without contributing to it. Worse, they expose society to devastating harm by building critical infrastructure with open-source code without assuring its security.

The community is spread too thin to solve the security problem on its own and the private sector's attention is elsewhere—in most cases, willfully blind to their security responsibilities. Too long has open source operated in the shadows. The government needs to bring open source to national focus and give it the priority and support it deserves as a core component of our critical infrastructure. Beyond that, the government needs to exercise its coercive power because without strong, direct regulation, the private sector lacks any incentive to amend its irresponsible practices and support the delivery of a critical resource.

But, unlike roads and bridges, we do not want to federalize open-source development. This robust community has self-governed for decades, innovating rapidly and providing immense value to society. It is already taking every measure to secure itself. Regulation's impact on the open-source community should be minimal in compliance and maximal in assistance to preserve this resource's unique potential to benefit society.

[530] About forty-three percent of cybersecurity experts polled by the *Washington Post* said that the United States is more vulnerable to cyberattacks now than it was five years ago. Marks, *The U.S. Isn't Getting Ahead*, *supra* note 34. About thirty-eight percent said that the United States is equally as vulnerable as it was five years ago. *Id.* Only nineteen percent said that the United States is less vulnerable than it was five years ago. *Id.* President Biden's top cybersecurity officials have also recently warned that "[m]ore frequent cyberattacks are the 'new normal' for U.S. companies and individuals." *Id.*