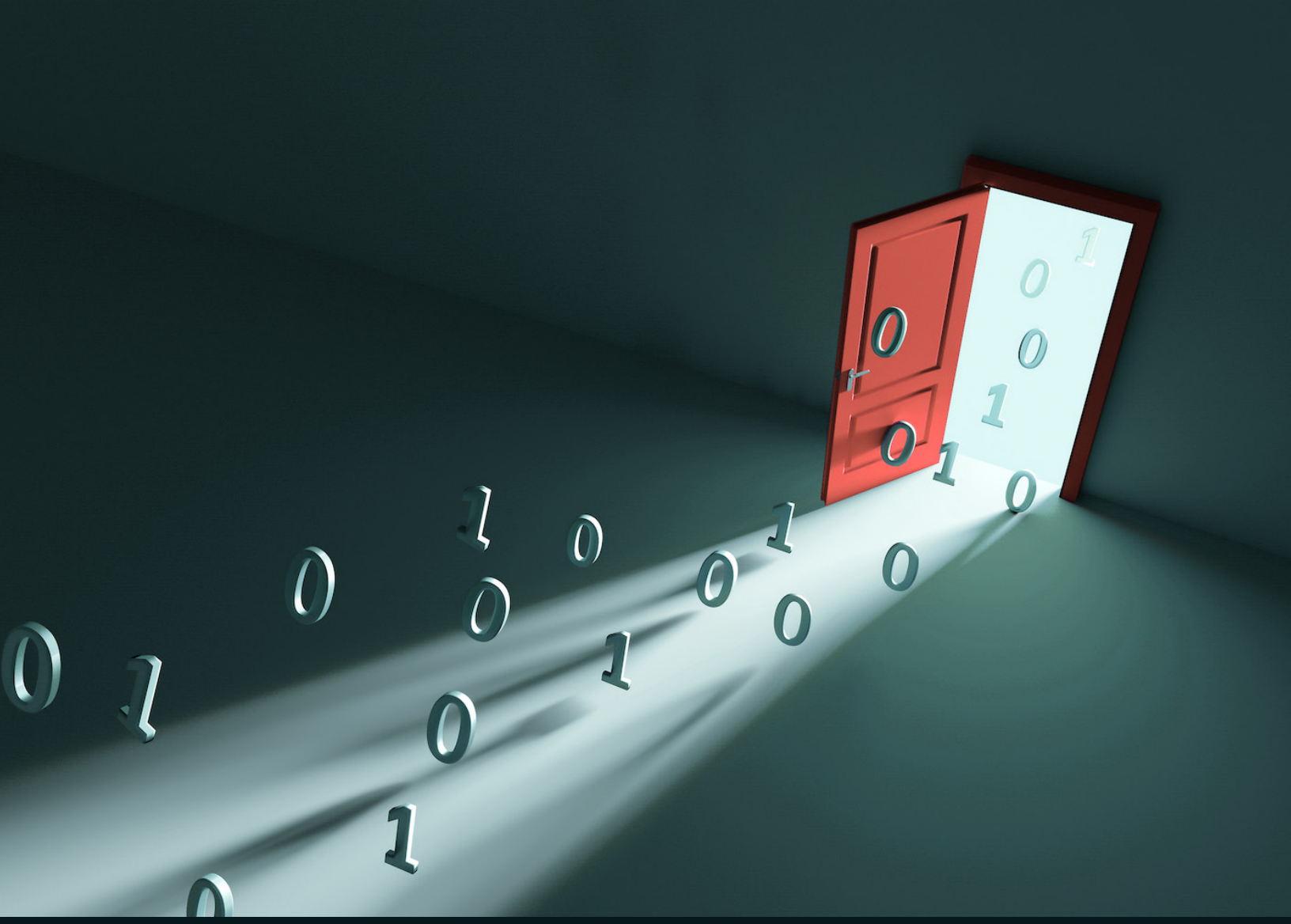


Securing Open Source Software at the Source

Creating a Center for Open Source Software Infrastructure and Security

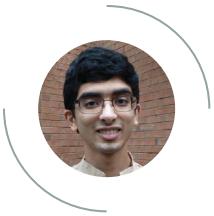
Ashwin Ramaswami

Plaintext Group
by SCHMIDT FUTURES

Friday, June 11, 2021
www.plaintextgroup.com

Securing Open Source Software at the Source

AUTHOR



Ashwin Ramaswami
Plaintext Group
Researcher

INDIVIDUAL ENDORSERS

Amotz Maimon
Schmidt Futures
Distinguished Engineering Fellow
Yahoo
(Former) Chief Architect

Bob Wyman
Google
(Former) Staff Software Engineer

Frank Nagle
Harvard Business School
Assistant Professor

Justin Dorfman
SustainOSS.org
Co-founder

Kumar Garg
Schmidt Futures
Managing Director and Head of Partnerships
Office of Science and Technology Policy
(Former) Assistant Director

Portia Burton
Document Write
Founder

Simon Handler
Atlantic Council
Assistant Director of the Cyber Statecraft Initiative

Tom Kalil
Schmidt Futures
Chief Innovation Officer
Office of Science and Technology Policy
(Former) Deputy Director for Policy

Trey Herr
Atlantic Council
Director of the Cyber Statecraft Initiative

All individual endorsers participated in their personal capacity. This report was prepared independently from any political or governmental entity. While the report generally reflects the observations, insights and recommendations of the group of endorsers, it is not the case that every endorser will agree with everything expressed herein.

Securing Open Source Software at the Source

EXECUTIVE SUMMARY

- Secure software supply chains are imperative to national security. When software supply chains come under attack, hackers and foreign adversaries compromise software to gain access to critical infrastructure, conduct espionage, and destroy information. As demonstrated by recent cyberattacks against SolarWinds and Microsoft Exchange, software supply chains are exposed and will continue to face assaults by nefarious actors unless the United States takes action to secure them.
- A critical foundation of both public and private software supply chains is open source software (OSS). In fact, approximately 98% of codebases1 contain OSS components.2 However, OSS is substantially supported by software engineers working on a volunteer basis who do not always prioritize security, potentially endangering our crucial software supply chains.

The federal government can play a greater role in safeguarding software supply chains by securing open source development in two ways:

1. Identifying and cataloging critical software in need of support; and
2. Funding critical improvements in open source software security.

These recommendations reflect Recommendation 4.1.1 of the Cyberspace Solarium Commission Report.[3]

As Congress prepares the upcoming FY 2022 National Defense Authorization Act (NDAA), one way to accomplish these recommendations is to include the establishment of a Center for Open Source Software Infrastructure and Security.

1 In software engineering, the codebase is the collection of source code used to build a software system — like the bricks of a building.

2 Synopsys, "2021 Open Source Security & Risk Analysis Report," https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2021.pdf

3 "Cyberspace Solarium Commission Report," March 2020, http://fdd.org/wp-content/uploads/2020/03/CSC-Final-Report.pdf

Securing Open Source Software at the Source

The Problem

Open source software is widely relied upon, but poorly supported, putting our national security at risk.

Like roads and bridges for the digital world, open source software (OSS) makes up much of our digital infrastructure and underlies many critical software systems, both public and private. Sometimes referred to as "free and open source software" (FOSS), OSS can be used, modified, and shared by the public according to its terms of distribution.[4]

The Rise of OSS

OSS usage is widespread and especially common in the private sector due to the relative benefits of OSS compared to proprietary software, such as innovation and convenience. The OSS operating system Linux — which is available for anyone to use and contribute improvements — is utilized by nearly 40% of all web servers.[5]

The federal government has also been on the cutting edge of OSS technology. In fact, by 2003, OSS was so commonly used in the Department of Defense (DoD) that one study by MITRE — a nonprofit that manages federally funded research and development centers for several federal agencies — determined the software was "vital to DoD information security" for its reliability and quality.[6]

Since then, OSS usage has grown substantially. A recent survey by the software company Synopsys found that more than 98% of audited codebases contained open source components, and 75% of all code was open source — an increase from 36% in 2015.[7]

Associated Risks

However, widespread adoption of OSS coincides with increased risks to software supply chain security. In 2014, the OSS library OpenSSL — a library maintained by volunteers that handles secure communications for 17% of servers across the Internet — disclosed the Heartbleed Bug, a vulnerability that exposed approximately 500,000 websites to exploitation.[8] In 2017, the consumer credit reporting agency Equifax announced a data breach caused by members of the Chinese People's Liberation Army — exposing the personal information of 147 million people and leading to a USD 425 million settlement[9] — through a weakness in the OSS web hosting framework Apache Struts.[10] According to the Cybersecurity and Infrastructure Security Agency (CISA), two of the top ten routinely exploited information-technology vulnerabilities were related to OSS as of 2020.[11]

OSS-related vulnerabilities have become so acute that members of the House Energy and Commerce Committee raised the issue in a 2018 letter to the

4 For a full definition of "open source software," see Appendix A of the Federal Source Code Policy, https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

5 "Usage statistics of Linux for websites," https://w3techs.com/technologies/details/os-linux

6 The MITRE Corporation, "Use of Free and Open-Source Software in the U.S. Department of Defense," Jan. 2, 2003, https://dodcio.defense.gov/Portals/0/Documents/FOSS/dodfoss_pdf.pdf

7 Synopsys.

8 Netcraft, "Half a million widely trusted websites vulnerable to Heartbleed bug," Apr. 8, 2014, https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

9 FTC, "Equifax Data Breach Settlement," Jan. 2020, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

10 Brian Barrett, "How 4 Chinese Hackers Allegedly Took Down Equifax," Feb. 10, 2020, https://www.wired.com/story/equifax-hack-china/

11 CISA, "Top 10 Routinely Exploited Vulnerabilities," May 12, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-133a

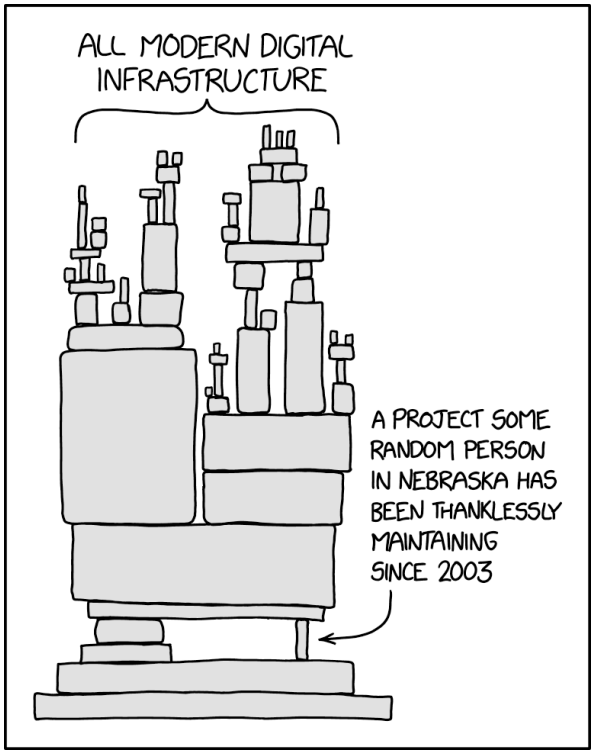
Linux Foundation, questioning the security and sustainability of the OSS ecosystem.[12] President Biden's May 2021 Executive Order on Improving the Nation's Cybersecurity also noted the importance of understanding the provenance of OSS in software supply chains.[13]

Lack of Security Resources

One of the primary reasons for these vulnerabilities is that OSS is often maintained by volunteers who do not always prioritize security, putting much of the Internet and millions of citizens at risk of attack. While some OSS projects are well-resourced by companies and non-profit organizations, other OSS code is maintained and released by people who struggle to monetize their work.[14]

According to a 2020 study by the Linux Foundation and the Laboratory for Innovation Science at Harvard, security fixes were among the external contributions that unpaid open source maintainers most desired, but among the areas where external contributors have the least interest to contribute. Maintainers would rather spend their volunteer time working on features or enhancements rather than security, which they described in terms such as "soul-withering chore."[15] Moreover, 44% of open source maintainers surveyed in 2018 said that they have never conducted a security audit of their code.[16] The report concluded that "financial contributions to support FOSS development could be highly beneficial to increase their security and sustainability if primarily directed toward specific purposes."[17]

When even closed source software developed by companies suffer supply chain attacks, such as the 2021 Microsoft Exchange attack and 2020 SolarWinds attack, it is all the more important to ensure open source has sufficient support. **We wouldn't rely solely on private companies and philanthropies to maintain and secure our roads and bridges that are open to the public; why would we do so for open source software?**



The state of open source (Credit: XKCD)

12 Greg Walden and Gregg Harper. "Letter to Mr. Zemlin," https://web.archive.org/web/20180422034612/https://energycommerce.house.gov/wp-content/uploads/2018/04/040218-Linux-Evaluation-of-OSS-Ecosystem.pdf

13 The White House, "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

14 James Turner, "Open source has a funding problem," Jan. 7, 2021, https://stackoverflow.blog/2021/01/07/open source-has-a-funding-problem/

15 The Linux Foundation and The Laboratory for Innovation Science at Harvard, "2020 FOSS Contributor Survey Report," https://www.linuxfoundation.org/wp-content/uploads/2020FOSSContributorSurveyReport_121020.pdf

16 Liran Tal, "Open source maintainers want to be secure, but 70% lack skills," Feb. 26, 2019, https://snyk.io/blog/open source-maintainers-want-to-be-secure-but-70-lack-skills/

17 The Linux Foundation and The Laboratory for Innovation Science at Harvard.

The Solution

The U.S. federal government must take action to better catalogue and fund the open source software ecosystem.

The United States needs to better secure its OSS supply chain at its source, or risk future attacks as OSS adoption increases and nefarious actors become more sophisticated.

The federal government can play a greater role in safeguarding software supply chains by securing open source development in two ways: 1) identifying and cataloging critical software in need of support, and 2) funding critical improvements in open source software security.

Recommendation 1: Identify and catalog critical software in need of support

Congress should initiate an effort to systematically identify the most critical open source software components and develop criteria for determining the criticality and vulnerability of open source software. This effort can be coordinated with CISA, through the National Risk Management Center (NRMC), to determine the open source software components most important to the nation's critical infrastructure sectors and National Critical Functions.[18] This effort should also engage NIST to determine guidelines for the criticality and vulnerability of open source software, creating criteria analogous to the Common Vulnerability Scoring System (CVSS).[19] The effort should result in an ongoing catalog that could be made available to other agencies as well as the public, analogous to the National Vulnerability Database (NVD) program.[20]

The effort for cataloging critical OSS could also build on existing work from (and involve collaborations with) related initiatives such as the Core Infrastructure Initiative's Census Program[21] and the OpenSSF's Criticality Score project.[22] Criteria for determining criticality and vulnerability could include: number of users of the OSS, code complexity of the system, number of full-time developers already working on the open source library, usage among federal or local government agencies, and usage in U.S. infrastructure sectors. Such criteria should also include "consumption patterns" such as how frequently packages are updated, the last time packages were downloaded, and the number of downloads of particular open source dependencies.

Recommendation 2: Fund critical improvements in open source software security

Congress should establish a process for funding OSS components that are determined to be both critical and in need of support, as well as improvements to the general ecosystem. Such funding could include:

- **An emergency fund that supports short-term and narrowly scoped security work**, such as

18 National Critical Functions (NCFs) define functions of government and the private sector that represent the most strategic risks of the nation. See: CISA, "National Critical Functions," https://www.cisa.gov/national-critical-functions

19 CVSS is a framework for describing the characteristics and severity of software vulnerabilities. See: NVD, "Vulnerability Metrics," https://nvd.nist.gov/vuln-metrics/cvss

20 NVD is a U.S. government database of vulnerability data that is available to the public. See: NIST, "National Vulnerability Database (NVD)," https://www.nist.gov/programs-projects/national-vulnerability-database-nvd

21 The Census Program identifies commonly used free and open source software components and examines them for vulnerabilities. See: "Vulnerabilities in the Core," https://www.coreinfrastructure.org/wp-content/uploads/sites/6/2020/02/census_ii_vulnerabilities_in_the_core.pdf

22 The Criticality Score is an effort to rate open source projects based on how critical they are to the entire community. See: Google Open Source Project, "Finding Critical Open Source Projects," https://opensource.googleblog.com/2020/12/finding-critical-open-source-projects.html

bug bounty programs for finding high-severity vulnerabilities or grants for fixing particularly critical vulnerabilities or hardening specific software. For example, qualifying grant proposals could be similar in nature to the Django Fellowship, which helped hire full-time developers to focus on triaging bugs and managing security releases for the open source web framework Django.[23]

- **A fund for non-software-related strategic initiatives or research** that may improve the security health of the entire open source ecosystem. For example, this could include events to improve education around security practices in the OSS ecosystem or research initiatives to better understand how open source developers approach dependency management.

The agency administering funding should publish clear criteria for the basis under which funding is awarded, and applicants should demonstrate their conformance with these criteria in order to be considered for grants. The results of the critical OSS catalog could also be used to better inform which types of projects and issues are prioritized in the funding and grantmaking process.

Mechanism of Implementation

One way to accomplish these two recommendations is for Congress to create a Center for Open Source Software Infrastructure and Security, which could be included in the upcoming FY 2022 National Defense Authorization Act (NDAA).

As outlined in the bipartisan Cyberspace Solarium Commission Report[24], one place to house such a Center would be under the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Homeland Security Advanced Research Projects Agency (HSARPA).

The Center could build on the agency's work in promoting OSS through the Homeland Open Security Technology (HOST) program[25] and its existing grantmaking capacity, and could attract top talent from the cybersecurity sector to focus resources on better improving OSS infrastructure.

Another potential agency that could house the Center is the Cybersecurity and Infrastructure Security Agency (CISA), as its primary mission is to enhance the security, resiliency, and reliability of the nation's cybersecurity and communications infrastructure.

Establishment and funding for this Center could be added as an amendment to the FY 2022 NDAA, stating clearly as a mandate in the statutory text the two recommended goals outlined above.

Support for Public Investment

Mechanisms for public and philanthropic funding of critical OSS are already in place. The above two recommendations would build on CISA's recent decision to invest in the open source election auditing software tool Arlo.[26] The European Commission's FOSSA (in 2014) and FOSSA 2 programs (in 2020) also funded both an inventory of critical OSS infrastructure[27] and a bug bounty program that successfully fixed dozens of critical or high OSS

23 Tim Graham, "Django Fellowship Program: 2016 retrospective," Dec. 28, 2016, https://www.djangoproject.com/weblog/2016/dec/28/fellowship-2016-retrospective/

24 "Cyberspace Solarium Commission Report," March 2020, http://fdd.org/wp-content/uploads/2020/03/CSC-Final-Report.pdf

25 "Homeland Open Source Technology Fact Sheet," July 29, 2015, https://www.dhs.gov/publication/ST-homeland-open-source-technology

26 CISA, "CISA Invests in Cutting-Edge Election Security Auditing Tool Ahead of 2020 Elections," Nov. 21, 2019, https://www.cisa.gov/news/2019/11/21/cisa-invests-cutting-edge-election-security-auditing-tool-ahead-2020-elections

27 European Commission, "EU-FOSSA 2 Deliverables," https://joinup.ec.europa.eu/collection/eu-fossa-2/eu-fossa-2-deliverables

vulnerabilities.[28] Moreover, the Ford Foundation and Sloan Foundation's Critical Digital Infrastructure Research Fund[29] and the Chan Zuckerberg Initiative's Essential Open Source Software for Science have supported open source software maintenance and research through a grant program.[30] A Center for Open Source Software Infrastructure and Security would build on such initiatives, but with greater scale and impact.

Public funding of open source has a track record of significant return on investment. Much of the technologies underpinning the Internet, including the widely-used open source Apache Web Server, were enabled only by an initial investment by NSF into the development of NCSA HTTPd decades ago.[31] Additionally, the investment by the World Bank's Global Facility for Disaster Reduction and Recovery (GFDRR) and its partners in the open source geospatial project GeoNode was conservatively estimated to give a 200% return on investment, in addition to creating a "thriving, mutually beneficial ecosystem" of individuals, government agencies, and private entities.[32] Moreover, public support of OSS has been shown to lead to substantial increases in jobs in the IT sector.[33]

These recommendations have broad support across the aisle. These recommendations directly follow from the bipartisan Cyberspace Solarium Commission Report. Moreover, similar proposals for public funding of OSS have also been included in a 2020 Brookings Institution article[34] and a March 2021 Atlantic Council report calling for a federal "open-source security evangelism and support office."[35]

Conclusion

Securing and strengthening software supply chains is a national security and economic priority. The United States must prioritize greater open source security by cataloguing and funding the ongoing maintenance of critical open source projects. By establishing a Center for Open Source Software Infrastructure and Security in the FY 2022 NDAA, Congress has an opportunity to strengthen our digital infrastructure, prevent future cyberattacks, and safeguard all American citizens.

28 European Commission, "EU-FOSSA 2 - the EU's open source cybersecurity project ends," July 14, 2020, https://ec.europa.eu/info/news/eu-fossa-2-eus-open-source-cybersecurity-project-ends-2020-jul-14_en

29 Ford Foundation, "Critical Digital Infrastructure Research," https://www.fordfoundation.org/campaigns/critical-digital-infrastructure-research/

30 Chan Zuckerberg Initiative, "Essential Open Source Software for Science," https://chanzuckerberg.com/eoss/

31 Shane Greenstein and Frank Nagle, "Digital Dark Matter and the Economic Contribution of Apache," Oct. 2013, Research Policy, 43(4), 623-631, https://doi.org/10.1016/j.respol.2014.01.003

32 GFDDR, "Open Data for Resilience Initiative & GeoNode: A Case Study on Institutional Investments in Open Source," 2017, https://opendri.org/wp-content/uploads/2017/03/OpenDRI-and-GeoNode-a-Case-Study-on-Institutional-Investments-in-Open-Source.pdf

33 Frank Nagle, "Government Technology Policy, Social Value, and National Competitiveness," Mar. 21, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355486

34 Frank Nagle, "Why Congress should invest in open source software," Oct. 13, 2020, https://www.brookings.edu/techstream/why-congress-should-invest-in-open source-software/

35 Trey Herr, et al., Mar. 29, 2021, "Broken trust: Lessons from Sunburst," https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst