GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

April 2, 2018

Mr. Jim Zemlin
Executive Director
The Linux Foundation
1 Letterman Drive
Building D, Suite D4700
San Francisco, CA 94129

Dear Mr. Zemlin:

We write to you today in support of open-source software (OSS) and to request your assistance in gaining a deeper understanding of the current state of the ecosystem. As the last several years have made clear, OSS is such a foundational part of the modern connected world that it has become critical cyber infrastructure. As we continue to examine cybersecurity issues generally, it is therefore imperative that we understand the challenges and opportunities the OSS ecosystem faces, and potential steps that OSS stakeholders may take to further support it.

In April 2014, researchers publicly revealed details about a critical cybersecurity vulnerability they termed "Heartbleed" in the open-source software (OSS) programming library OpenSSL, which at the time was installed in an estimated sixty percent of all websites.[1] As the Heartbleed vulnerability enables the theft of sensitive information from unpatched systems and is simple to exploit, this disclosure immediately set off a widespread scramble as affected organizations raced to update their systems before malicious actors could leverage the flaw. While many organizations succeeded in doing so, others did not; at least three cited the Heartbleed vulnerability as the root cause of later cybersecurity incidents, including the compromise of 4.5 million patient records from one health care provider.[2]

[1] Dan Goodin, *Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping*, ARS TECHNICA (Apr. 7, 2014), https://arstechnica.com/information-technology/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eavesdropping/.

[2] *CHS Hacked via Heartbleed Vulnerability*, TRUSTEDSEC (Aug. 19, 2014), https://www.trustedsec.com/2014/08/chs-hacked-heartbleed-exclusive-trustedsec/; Pete Evans, *Heartbleed bug: RCMP asked Revenue Canada to delay news of SIN thefts*, CBC NEWS (Apr. 14, 2014), http://www.cbc.ca/news/business/heartbleed-bug-rcmp-asked-revenue-canada-to-delay-news-of-sin-thefts-1.2609192; Leo Kelion, *Heartbleed hacks hit Mumsnet and Canada's tax agency*, BBC (Apr. 14, 2014),

The widespread impact of the Heartbleed vulnerability through the deployment of a piece of OSS forced individuals and organizations outside of the information technology community to recognize what members within the community had long-known: software is no longer written, but assembled. Software libraries that reliably handle basic programming staples such as transport-layer encryption, network time management, or data storage are available through the OSS ecosystem, providing organizations which leverage them a solid foundation upon which they may then build their own unique products.[3] As such, many organizations include OSS in their code, with one survey estimating that 78 percent of companies "run on open source."[4] As a result of this widespread adoption, OSS has become critical cyber infrastructure, and the sustainability and stability of the OSS ecosystem is essential to the sustainability and stability of organizations' cybersecurity generally.

While the extent of OSS adoption clearly demonstrates the value that the ecosystem provides, its pervasiveness also creates widespread, distributed, and common points of potential risk across organizations when OSS vulnerabilities are found. This is a hard lesson that society has arguably already learned; vulnerabilities in Microsoft's Windows operating system, Adobe's Flash Player, or Apple's macOS, for example, create similarly widespread points of common risk when vulnerabilities similar to Heartbleed are found in these proprietary pieces of software, as well.[5] However, companies like Microsoft, Adobe, or Apple have the processes and procedures in place to quickly address these vulnerabilities, and—more importantly—the time and funding to do so. This is not always the case for OSS vulnerabilities, as OSS creators or maintainers may be globally-located volunteers, who often have unrelated full-time employment and may be uncompensated for their OSS work.

As Executive Director of the Linux Foundation, which organizes the Core Infrastructure Initiative (CII), this is a reality of which you are aware. The CII was established in the aftermath of Heartbleed in recognition of this very fact, and is "a multi-million dollar project to fund and support critical elements of the global information infrastructure."[6] As of 2016, the CII had provided $1,945,000 in total funding to more than 14 OSS projects and initiatives, with the first

http://www.cbc.ca/news/business/heartbleed-bug-rcmp-asked-revenue-canada-to-delay-news-of-sin-thefts-1.2609192.

[3] *2016 Future of Open Source Survey Results*, BLACK DUCK SOFTWARE (Apr. 25, 2016), https://www.slideshare.net/blackducksoftware/2016-future-of-open-source-survey-results, (slide 13).

[4] *2015 Future of Open Source Survey Results*, BLACK DUCK SOFTWARE (Apr. 15, 2015), https://www.slideshare.net/blackducksoftware/2015-future-of-open-source-survey-results/9-SECTION2CORPORATEUSE2XSINCE_2010USE_OF_OPEN_SOURCE.

[5] *See e.g.*, John E. Dunn, *The greatest security story never told – how Microsoft's SDL saved Windows*, TECHWORLD (Mar. 6, 2014), https://www.techworld.com/news/security/greatest-security-story-never-told-how-microsofts-sdl-saved-windows-3505545/; Dan Goodin, *An Adobe Flash 0day is being actively exploited in the wild*, ARS TECHNICA (Feb. 2, 2018), https://arstechnica.com/information-technology/2018/02/theres-a-new-adobe-flash-0day-and-up-and-coming-hackers-are-exploiting-it/; Shaun Nichols, *Pro tip: You can log into macOS High Sierra as root with no password*, THE REGISTER (Nov. 28, 2017), https://www.theregister.co.uk/2017/11/28/root_access_bypass_macos_high_sierra/.

[6] *FAQ – What is the Core Infrastructure Initiative?*, CORE INFRASTRUCTURE INITIATIVE (last visited Jan. 17, 2018), https://www.coreinfrastructure.org/faq.

being OpenSSL – the OSS library that contained the Heartbleed vulnerability.[7] CII's funding has enabled these OSS projects and initiatives to undertake audits to root out vulnerabilities before they are found and exploited, develop tools for code analysis and testing, create a best practices program that helps educate OSS developers and encourage secure coding practices.[8]

The Committee appreciates the work that the CII, its sponsors, and the various projects and developers that it supports have accomplished. The OSS ecosystem is more sustainable and more stable due to these efforts, which directly increases the sustainability and stability of the cybersecurity of organizations that rely on OSS, as well. More work remains to be done, however. OSS adoption will continue to grow, making the sustainability and stability of the OSS ecosystem even more vital.

To assist us in gaining a deeper understanding of the current state of the OSS ecosystem, and pursuant to Rules X and XI of the House of Representatives, we ask that you respond to the following questions by no later than April 16, 2018:

1. Has the CII performed a comprehensive study of which pieces of OSS are most critical to the "global information infrastructure"?

    a. If not, does the CII plan to perform such a study?

    b. What would the CII need in order to do so?

2. Has the CII, or any other organization, compiled any statistics on OSS usage?

    a. If not, does the CII plan to perform such a study?

    b. What would the CII need in order to do so?

3. In your estimation, how sustainable and stable is the OSS ecosystem?

4. Based on your response to the previous question, how can the OSS ecosystem be made more sustainable and stable?

We appreciate your attention to this request. If you have any questions, please contact Jessica Wilkerson of the Majority Committee staff at (202) 225-2927.

[7] *Core Infrastructure Initiative 2016 Annual Report*, CORE INFRASTRUCTURE INITIATIVE 13 (Jan. 11, 2017), https://www.coreinfrastructure.org/sites/cii/files/cii_annualreport_2016_fnl_digital.pdf.
[8] *Id* at 14-19.

Sincerely,

Greg Walden

Greg Walden
Chairman

Gregg Harper

Gregg Harper
Chairman
Subcommittee on Oversight
and Investigations

cc: The Honorable Frank Pallone, Jr., Ranking Member

The Honorable Diana DeGette, Ranking Member
Subcommittee on Oversight and Investigations