THE LINUX FOUNDATION

April 23, 2018

Honorable Greg Walden
Chairman
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Honorable Gregg Harper
Chairman
House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
2227 Rayburn House Office Building
Washington, DC 20515-6115

I would first like to thank the Energy and Commerce Committee and the Subcommittee on Oversight Investigations, Chairman Greg Walden, Subcommittee Chairman Gregg Harper and the members of the Subcommittee for inviting The Linux Foundation to comment on the current state of Open Source Software ("OSS").

The Linux Foundation (the "LF") believes nearly every person, business, institution and government in the world depends on OSS and that ensuring the security of this critical resource is a matter of utmost importance and collective responsibility. Although we believe software security concerns apply equally to OSS and "closed source" software, our organization is uniquely positioned to lead an overarching OSS security effort and given the increased nature of global cyber security threats, we know that our work is more important than ever.

All of us at the LF appreciate the Committee's outreach, shared interest in this work, and the opportunity to respond to your thoughtful, insightful and important questions. We hope our response will help further the Committee's appreciation for our deep commitment to cyber security, OSS developers, and a thriving OSS ecosystem[1].

About The Linux Foundation

The LF is a 501(c)(6) nonprofit organization founded in 2000 and is home to the Linux kernel, the world's most widely deployed software, which underpins the vast majority of modern computing

[1] OSS ecosystems include developers commercial product and solution providers and end users who deploy OSS in their systems applications and infrastructure

systems including most smartphones, most public cloud services, many Internet-of-Things (commonly referred to as “IoT”) devices, and all of the world’s top supercomputers[2]. Today, the LF has expanded its work far beyond the Linux operating systems and is engaged in multiple projects across all major core technologies from infrastructure to applications to devices.

The LF’s mission is to support the development of sustainable OSS projects – from artificial intelligence to cloud to blockchain – and the developer communities that build these projects. We advance our mission by supporting the brilliant developers working on various OSS projects and providing them with required infrastructure to support their technological developments, legal needs, events, and training programs that help OSS communities effectively collaborate and prosper.

The LF’s operations and resources are funded by the LF’s members, which include most of the largest technology firms in the world, such as Cisco, Google, IBM, Intel, and Microsoft, in addition to over 1,000 of the world’s leading solution providers and end user companies that deploy a wide variety of OSS and closed source components within their production systems. Other than two top Linux kernel maintainers, the LF does not directly employ the software developers that contribute source code to the OSS projects it hosts. Rather, thousands of developers either work for other organizations, including the majority of Fortune 500 companies, or developers contribute independently as individuals. This neutral structure is important because it ensures that the companies benefiting from OSS are also contributing to it through the funding of their developers.

The LF has a long-standing track record of successfully building broad support and funding for resources required to accelerate and sustain collaboration amongst solution providers, users of OSS, academic and other organizations. The LF is not alone in this effort as there are other OSS nonprofit foundations (e.g., the Apache Software Foundation and the Eclipse Foundation) in addition to the many OSS project communities that we engage and partner with, but which are not necessarily nonprofit entities. The end result of this open collaborative process, both at the LF and elsewhere, has produced the broadest, most successful, ambitious and groundbreaking investment, expansion, creation and maintenance of shared technologies in the world.

Open Source Software is Ubiquitous and Here to Stay

The multi-decade progression toward the adoption and continual use of OSS in developing modern technological products, solutions and services is permanent and irreversible. The majority of the world's economic systems, stock exchanges, the Internet, supercomputers and mobile devices run the open source Linux operating system and its usage and adoption continue to expand. Billions of individuals

[2] https //www top500 org/statistics/details/os am/1 using the latest data (November 2017)

may not know they're using OSS every day, but their modern television, smart watch, camera, automobile and smartphone rely on OSS. Today a modern automobile contains more software source code than an F-35 fighter jet.[3] In order to enable this mass production of software and a thriving technology industry, industry long ago recognized that the value of collective, open collaborative development through OSS was critical. It is estimated that the vast majority of source code in any modern software implementation across most sectors is comprised of OSS.[4] This groundbreaking collaboration allowed for the rapid advancement of technology in the United States and beyond and helped position the US as a global technology leader.

The OSS development model succeeds because software developers openly develop software in collaboration with other contributors from around the world. In that way, the development of OSS can most easily be compared to the advancement of science, where the underlying software infrastructure, like the basic science of each discipline, is developed collaboratively and iteratively by coordinating, distributed experts over time. The best minds in the world come together to build the strongest technical solution, regardless of their company affiliation. The software is available to anyone in the world to view, use, modify and redistribute under the terms of an OSS license[5]. These developers and the organizations employing them contribute their expertise and intellectual property to advance their own interests, but together with others acting in a similar model, they collectively create some of the world's most important software.

It is important to note that there is no other way to create the sheer volume of software required to enable today's digital economy without widespread joint software development efforts and code reuse policies. The intellectual property model for OSS is the only viable and proven means to collaborate at scale. Access to freely available, high quality software worth billions of dollars is what has enabled the Internet to flourish in a way that would have been impossible if any single organization or company had tried to create this software on its own. Therefore, it is a collective responsibility – and imperative – for business, industry, academic and technology leaders to work together to ensure that OSS is written, maintained and deployed as securely as possible. It is essential that the corresponding OSS communities are supported and properly enabled to be proactive enough to manage future security challenges that will arise over time.

Open Source Software, Security and Code Development

Due to the nature of the LF's work in leading OSS collaboration efforts, our focus is, and has been on security across all platforms. The LF is working on the front lines of enhanced security by engaging

[3] https //informationisbeautiful net/visualizations/million-lines-of-code/

[4] https //blog blackducksoftware com/spotlight-on-open-source-appdev-preeminence-driving-change

[5] https //opensource org/osd

industry leaders and OSS developers who have the technical expertise to know what to do, both before and after security challenges arise. There are three key components to how OSS security and code development come together:

1. Code Flows - Upstream and Downstream: It is important to understand how code "flows" in the global software supply chain. "Upstream" refers to the original OSS that is developed. It is then integrated and deployed into commercial "downstream" products such as a mobile phone, or in civil infrastructure such as our modern telecommunications or energy systems. Commercial companies downstream are responsible for the products and services they provide but are dependent on upstream OSS code without which they could not exist. This matters because a more secure upstream source of OSS code will increase security of downstream infrastructure, products and services. It is also critical that fixes downstream get contributed back upstream where they can benefit other members of the ecosystem.

2. Commercial Use of OSS: When discussing security and OSS it's important to keep in mind that the expertise regarding the software resides in individuals, companies and organizations around the world. Most of the people familiar with securing systems are employed by commercial companies that provide solutions and support for the software in a product or service. Most commercial software leverages both OSS and closed source components. The decisions about which OSS components to use are determined by developers and security experts employed by the vendors and operators that use, distribute, and support commercial software products and services. The LF's key role lies in facilitating the coordination amongst the global organizations that employ these resources and enabling widespread collaboration.

3. OSS Project Variance: It is equally important to understand that the software components these expert developers are using and combining come from various OSS projects that differ in scope, complexity and size. OSS projects may comprise a simple codebase that fulfills one basic function, or an OSS project could provide a full telecommunications platform that comprises millions of lines of source code. Some OSS projects may have thousands of developers contributing and maintaining the corresponding codebases, whereas other OSS projects may have just a single individual working on the codebase. One critical concern to the LF is that many developer communities working on OSS projects do not have enough security experts that are contributing to or maintaining the codebases. As a result, there is a great deal of variance between individual OSS projects regarding the security framework, practices, and tools that are available to the developers of the corresponding OSS communities.

The Linux Foundation's Commitment to Security - Core Infrastructure Initiative (CII)

The LF is focused on leveraging the collaborative development model underlying OSS to improve security across all OSS projects. We believe that private sector investments driven by commercial interests can provide sustainable improvements in the collective security of OSS projects. That is why we created and established the LF’s Core Infrastructure Initiative (“CII”)[6].

The CII is a top group of experts from various organizations who work together to:

1. identify the most critical OSS projects by industry verticals and the risk they present to industry and society as priorities in our actions;
2. define practical steps that improve the security of the identified OSS projects while being broadly applicable to other OSS projects;
3. foster a culture of security in OSS communities by disseminating security best practices and rewarding proactive communities with badges; and
4. deploy strategic investments in areas such as tooling and research that broadly and holistically increase the security of all OSS projects.

Census I & the CII Best Practices Badge

In 2015 the LF undertook an initial census of the OSS commonly used in enterprise infrastructure under the CII umbrella program. The goal of this census is to focus on remediation of the projects that are the most widely deployed yet lack basic resources to maintain and secure their software code. CII is taking important steps to identify and promote security development best practices in the OSS communities. Over 1,400[7] OSS projects have followed the LF’s lead and have either completed or are working on defining their security practices and earning the right to display a unique badge that establishes and proves the project’s commitment to security.[8] While this may seem like a large number of projects, we would like to leverage CII to significantly increase the number of badged projects. One means to achieve this we are considering is to promote the use of the badge as a key criteria for industry selection of which OSS packages they are willing to deploy on their systems.

The Security Case For Greater Software Transparency

It is critical for anyone appraising the value of OSS to understand that any software or system security cannot be evaluated or maintained if you do not know what the software or system contains or pulls in

[6] https //www corein rastructure org/

[7] https //bestpractices corein rastructure org/en/projects

[8] https //www corein rastructure org/programs/badge-program

as a dependency. Software utilizing various OSS components cannot be updated to incorporate key security patches if no one knows where the affected OSS components are in use or which distribution channels they originated from.

Openness and transparency in software do not inhibit security, but rather, transparency enables better security overall – better peer review of upstream source code and improved downstream collective response.

SPDX

The LF has also introduced a cross-industry program to improve visibility into what open source projects are in use called the Software Package Data eXchange ("SPDX"). The SPDX specification and its associated data formats and openly available tools enable companies and projects to produce and exchange a human and machine-readable bill of material ("BoM") for software products and packages.[9] The SPDX package level specification permits inclusion of a link to the Common Platform Enumeration (commonly referred to as the "CPE") from NIST[10]. With a SPDX BoM, anyone can identify current and future Common Vulnerability Enumeration[11] ("CVEs") and Common Weakness Enumeration[12] ("CWEs") associated with the package CPE by using public data from the NIST National Vulnerability Database[13].

If SPDX had been in widespread use when the Heartbleed[14] bug in OpenSSL was publicly disclosed in 2014, organizations would have been able to search their BoMs and immediately know where pre-patch packages of OpenSSL were in use in their software systems. This immediate insight would have enabled those organizations to make sure that each instance was updated with the latest security patch. Without efficient access to this information, it took weeks or months for many organizations to identify all of the copies of OpenSSL code that needed to be patched.

[9] https //spdx org/ he SPDX speci ication was originally created to assist so tware suppliers and their customers to exchange very granular data on which OSS components were included in a bill o materials delivered through the supply chain By having a common standard the OSS packages included in the bill o materials enabled instant machine-readable access to what so tware packages were in use Within an industry adoption o SPDX could allow or a rapid response ecosystem whereby security issues and the potential targets could be rapidly identi ied and monitored until patched with a security ix

[10] https //spdx org/spdx-speci ication-21-web-version#h hb0u4akk190q

[11] https //nvd nist gov/vuln

[12] https //samate nist gov/BF/Enlightenment/CWE html

[13] https //nvd nist gov/

[14] From http //heartbleed com " he Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic so tware library his weakness allows stealing the in ormation protected under normal conditions by the SSL/ LS encryption used to secure the nternet SSL/ LS provides communication security and privacy over the nternet or applications such as web email instant messaging and some virtual private networks (VPNs)

he Heartbleed bug allows anyone on the nternet to read the memory o the systems protected by the vulnerable versions o the OpenSSL so tware his compromises the secret keys used to identi y the service providers and to encrypt the tra ic the names and passwords o the users and the actual content his allows attackers to eavesdrop on communications steal data directly rom the services and users and to impersonate services and users "

As of January 2017, nearly 3 years after the Heartbleed public disclosure, over 200,000 public internet-facing devices were still unpatched for this critical vulnerability.[15] As of February 2018, Synopsys conducted a similar analysis and found over 137,000 public internet-facing devices were still unpatched. These statistics do not even include the servers, embedded systems and other non-public, connected devices behind firewalls and internal networks.

This pattern of vulnerability is not unique to OpenSSL. It's also not unique to OSS, as many closed source systems face the same challenges enabling downstream users to patch their systems. For example, on March 9, 2017, Equifax was notified by US CERT to update their Apache Struts installations for a vulnerability that had already been fixed in the upstream Apache Struts project.[16] On March 15, 2017, Equifax teams ran internal scans that "did not identify the Apache Struts vulnerability".[17] From the available testimony, it is unclear if Equifax maintained a BoM for its systems that would have provided immediate access to where vulnerable software was used. In May of 2017, Equifax suffered a massive data breach, leaking over 145 million Americans' personal data, due to the previously notified vulnerability in the Apache Struts OSS project.[18]

The LF is now building on the SPDX format and hosting a cross-industry program called OpenChain to improve the processes which gather and exchange this data through a multi-vendor supply chain to the end user[19]. OpenChain offers the promise of delivering precise, machine-readable visibility into what OSS was used in software delivered from suppliers, giving the end product or solution organization much greater ability to act on security issues.

Building a Secure Future

The work of the LF to drive OSS development and enhance security is unique, focused and determined, but there is much more to be done if we are going to effectively tackle the very real and fast-growing challenges in the years to come.

Each of the LF's security projects under the CII are designed to support developers, industry and the people who use these products. In order to prioritize our efforts for all of this work, we are gathering and analyzing data about which OSS is most widely in use, its function, its source, and the processes

[15] https //www in oworld com/article/3162346/security/that-hearbleed-problem-may-be-more-pervasive-than-you-think html

[16] https //docs house gov/meetings/ F/ F17/20171003/106455/HHRG-115- F17-Wstate-SmithR-20171003 pd

[17] d

[18] d

[19] https //www openchainproject org/ For OSS we have communities defining compliance processes or supply chains OpenChain to deal with license compliance but these same programs could be extended to cover supply chain security risk management as well

deployed in its development. Industry participation and support for our efforts will be essential going forward.

LF Proactive Security Measures

The LF has created a foundation of critical work under the CII and is now focused on going further by placing a strong emphasis on proactive security. Our work must be directed towards addressing challenges and problems before they come to the surface and while the development of OSS is in process. The LF's vision for executing a proactive strategy is to provide:

1. Access to anonymized OSS usage data across major software supply chains;
2. Leverage information on the most widely used OSS projects in security critical industries to proactively identify OSS project communities that may be an issue in the future, and
3. Apply resources to weaker OSS project communities to prevent future issues.

OSS communities are often dynamic and fast paced ecosystems. Despite differences in opinions and ideas, technologists work together in these global communities every day to create incremental improvements to code that provides amazing technology. We know that we can successfully apply the same collaborative development model to address security shortcomings as a community and that we can effectively lead this effort, as we have done for the last nearly twenty years. We look forward to continuing our work with academic, commercial and national security and policy leaders to advance these short and long-term solutions together.

Given this background, here are our answers to the questions you asked.

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?**

The LF has been leading the way on OSS software development and security since its establishment in 2000. The LF employs the creator of the Linux operating system, Linus Torvalds, who is a global thought leader on OSS and has always been involved in remediating Linux security issues. Over the years we've also seen the number of security challenges scale with the massive increase in adoption of Linux and OSS. In 2015, we launched CII to move away from an issue-based, reactive mode to take a more proactive and holistic view of security across all OSS. The goal was to create an OSS security "heat map" for critical projects that pose the greatest risk to industry and society.

The LF CII then launched the Census Project[20] (which we will refer to here as “Census I”) in 2015 to create the first platform for identifying OSS projects that are widely deployed but under-resourced or otherwise at risk of inadequate maintenance. The LF considers this project an important first step, though limited in scope due to the financial resources and data available at the time.

The LF is advancing to Census II which will exponentially expand our “heat mapping” effort but additional resources are required to continuously expand the scope and maintain the relevance of the CII and its Census Projects. The greatest success in software security comes when we holistically review the operations throughout the entire ecosystem and surgically determine the specific challenge points that, when addressed properly, can greatly impact the larger system overall. This way, our energies can produce the greatest good and the longest-term benefits.

OSS code created in upstream[21] projects flows downstream through different global supply chains to be combined with other OSS projects, and often closed source software, into the final distributed software that provides end-product functionality. Addressing OSS security in the end-product will never be as effective as addressing the security practices in the upstream projects from which many other projects and products are built. The impact of improving the upstream projects before they flow downstream will benefit all end products that incorporate or are otherwise dependent upon the upstream project. Similarly, the quality of security that is built into the code as it originates upstream will be better than downstream product quality assurance “fixes” that may be constrained by choices and dependencies that are well established when the end-product is available for testing.

Key Background on Census I and the LF’s Advancement to Census II

Census I uses available data about OSS projects in a Linux distribution ecosystem, including the interdependencies of OSS projects upon each other. The scope of Census I is focused on OSS projects that are generally deployed in enterprise scenarios touching a network interface, as their network accessible nature presents a higher vulnerability risk. Census I leverages a community of security experts to develop a scoring methodology that is then applied to the project data to produce a relative score. Census I provides a clear list of projects that present the most risk. The enterprise technology companies funding the effort then applies the financial resources available to solutions that address challenges in the highest priority projects[22].

Census I is based on an enterprise IT scope of concern. It does not address consumer, embedded and industrial Internet of Things (“IoT) use cases, nor industry vertical use cases where stacks are being

[20] https //www coreinfrastructure org/programs/census-project

[21] https //en wikipedia org/wiki/Upstream (software development)

[22] https //www coreinfrastructure org/grants

developed, for instance, in the energy or telecommunications sectors. This is a critical area to better understand as more devices become “software defined” and there is more software controlling industrial and civil infrastructure systems. Over the last 20 years, the number of top 100 product and service companies that are software dependent has doubled to nearly 40 percent.[23] As more software is used to replace physical device systems or manual processes, the use of OSS as an underpinning for the stack becomes inevitable.

Census I funding and decision making is enterprise IT driven. The next phase - Census II - needs to be driven by security experts in the priority industries analyzed. The scope needs to also expand to cover commonly used systems where OSS is distributed. The decision makers and funders should also be different. There is a transition that will take resources to make, but which is nonetheless critical for our understanding and continuous improvement in the security of OSS and the global software supply chain.

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?**

The Linux Foundation understands the great value of data on OSS usage. To date, a comprehensive study of OSS usage and security risk has not existed. However, the LF, through its creation of the CII, in collaboration with the Institute for Defense Analyses (“IDA”), Synopsys and Laboratory for Innovation Science at Harvard University (“LISH”)[24] are designing the next generation of an OSS census (“Census II”), which will aim to evaluate widely deployed OSS package management systems, OSS project adoption in industry verticals and holistic research on the social and commercial ecosystems around those OSS projects.

Census II

The goal of the CII’s Census II is to leverage detailed data on the use of widely deployed OSS packages including by industry segments. Through this effort we can be more proactive and understand at a granular level which projects may present ecosystem security vulnerabilities. As with the initial Census I, Census II will apply analytics to score projects based on a risk profile. The results of Census II are intended to present clear guidance to industry and policy leaders as to which OSS

[23] https //www mckinsey com/business-functions/digital-mckinsey/our-insights/an-executives-guide-to-software-development

[24] L SH is an interdisciplinary research organization led by Professors Karim R Lakhani (Harvard Business School) and David Parkes (Harvard School of Engineering and Applied Science) focused on generating insights at the intersection of technology innovation and management Professor Lakhani is one of the leading scholars of open source software and has co-edited two volumes on open source and open innovation by M Press David Parkes is a leading computer scientist working at the intersection of computer science and market design

projects and communities present the greatest risk to their specific industries. This knowledge should guide investment of resources to drive secure coding practices in the identified OSS projects.

As part of the Census II comprehensive study, our current plan is that:

- Synopsys will provide access to data on the commonly used OSS projects by various industries.
- IDA will quantitatively identify the most important OSS projects among the millions managed by language-level package managers and, of those, identifying the ones most needing security-related investments.
- LISH will form a team of economists, computer scientists, and management scholars to create relevant research on ecosystem formation, growth and sustainability. The data from Synopsys and IDA will inform the scope of the software communities studied by LISH. LISH will evaluate the technical, commercial, managerial and social health of the OSS ecosystem around core projects.

Census II is still in a formative stage but is a critical effort for OSS security that no one else is undertaking. To continue to thrive, the CII and its Census II program will seek private sector funding and support. The availability of future funding and access to technical expertise will determine how comprehensive the results will be and, just as importantly, whether the results will represent a particular point in time or an ongoing analysis of emerging use trends and new areas of vulnerability. Data and financial support from industry, government and other sources will be critical to enabling us in applying an appropriate level of resources to this endeavor.

Table: Summary of Census I and Census II

	Census I	**Census II**
OSS Project Data Scope	OSS used in Linux distribution	OSS used broadly in application and systems in industry verticals
Risk Ranking Analysis	Quantitative analysis based on risk scoring	Quantitative analysis based on risk scoring
Research Scope	Not in scope	Technical, commercial, managerial and social health
Proactive Actions Enabled	Identify and strengthen weaker projects widely used in enterprise infrastructure	Identify weaknesses in package management systems and industry verticals

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

The OSS ecosystem is very strong and sustainable. The expansion of resources invested in OSS and exponential growth of the new projects and ubiquitous market adoption throughout the world are increasing rapidly. The economic model of upstream co-development, downstream value creation and subsequent upstream reinvestment in critical OSS projects is a fundamental shift in the “winner takes all” technology sector. Modern imperatives such as rapid time to market, global competition, and the move to a digital economy has created an environment where no single company or organization can create, source or maintain all the software they require on their own.

As companies around the world build solutions based on OSS, they and others like them invest new features, bug fixes and development efforts back into the upstream OSS project. If an organization does not contribute patches back upstream, it will fall out of sync with the upstream project and be forced to assume the cost of maintaining its own private version (a “fork”). This prospective maintenance cost is a strong incentive for organizations to contribute new features and fixes upstream into the source OSS project.

The natural economic incentive for organizations to contribute back to the projects provides sustainability and security because downstream users need to remain abreast of changes, updates, and fixes that ensure the security of OSS in all offerings. If there is a serious OSS project security failure, such as in the case of the Heartbleed vulnerability in OpenSSL, companies must be able to consume the communities’ responsive patches as quickly as possible.

OSS participants at times have embraced the aphorism, “*with many eyes, all bugs are shallow*.” This mantra means that open access to the source code also enables participants across the ecosystem to identify errors in the source code, also known as “bugs”, which are often the cause of security issues. This is not always the case for security vulnerabilities. For example, in the case of OpenSSL, prior to Heartbleed, a widely deployed piece of software was being maintained largely by the efforts of two individuals. However, since Heartbleed the industry has recognized this concern and made efforts to address this issue. Of course, even without these efforts, OSS code is, generally speaking, more secure from malicious and other security vulnerabilities than closed source code for which source is unavailable for scrutiny by others.

For example, a way to mitigate this problem is to develop metrics that can be used to define risk and sustainability in OSS communities. In 2017 the LF formed a project called the Community Health

Analytics Open Source Software ("CHAOSS")[25] project to understand how to measure which OSS projects are "healthy", meaning that they meet certain quantifiable metrics for being sustainable and stable[26]. The term 'healthy' describes an OSS project that is likely to continue producing secure, quality software through an active, diverse community of participants, including commercial solution providers who have incentives to contribute back upstream.

Understanding the health of individual projects is a requirement for improving the OSS ecosystem because health risks in one project often propagate to interdependent OSS projects or downstream projects. Through the CHAOSS project, we are able to apply basic, quantifiable risk metrics[27] to any OSS community project and inform the ecosystem dependent on those projects with an early warning signal before a stability or sustainability issue arises. Early detection, industry visibility and an ability to remediate security and sustainability issues quickly will be critical to securing OSS over the next decade or more.

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

In order to sustain and secure the OSS ecosystems, the LF must continue to lead through the CII, Census II and additional future security programs.

The LF would embrace a public-private partnership with the House Energy and Commerce and Appropriations Committees to further address these emerging challenges together including:

(1) identify the most critical OSS projects by industry and the risk they present to our collective security and privacy;
(2) define and underwrite practical steps that improve the security of these projects while being broadly applicable to other OSS projects;
(3) support and encourage the OSS community and industry in making strategic investments in areas such as tooling, training, rating and badging programs and research that broadly increase the security of all OSS;
(4) support and encourage the adoption of automated ways to track software BoMs across the global technology supply chain;
(5) consider financial and tax incentives to encourage industry to contribute to OSS development and security efforts; and

[25] https //www linux oundation org/blog/chaoss-project-creates-tools-to-analyze-so tware-development-and-measure-open-source-community-health/

[26] https //chaoss community/metrics/

[27] https //github com/chaoss/metrics

(6) create incentives for the government to adopt OSS projects based on security considerations, ratings, badging, etc.

In addition, the LF would welcome the opportunity to engage more directly and regularly with the House Energy and Commerce and Appropriations Committees, and other Congressional leaders with overlapping jurisdictions and interests in cybersecurity to work together, brief Congress on a regular basis and to work with the committee to draft comprehensive security plans and pilot projects that can advance our efforts.

It is essential that all policy and decision makers understand that we are all dependent upon the global software infrastructure and that infrastructure is comprised of millions of OSS projects that are developed and shared under various OSS licenses. In ten years' time, there is a high likelihood we will see millions of new OSS projects emerge.

The LF's CII and its Census I and II, best practices badge, SPDX, and CHAOSS were all formed to improve the security landscape of OSS. We are seeking scalable ways to communicate best practices from the experts out to a broad base in the OSS ecosystem. The proposed actions above are designed to address what the LF sees as the next steps in our journey to secure software used across platforms and sectors around the world. As we progress we would welcome Congress' support and assistance in building alliances with organizations outside the LF's sphere of influence, particularly in industries where security is of highest importance.

Companies that directly or indirectly use the projects highlighted in our Census are often willing to devote resources to OSS projects they depend on in their solutions, but the skills required to perform many of these tasks are sometimes relatively rare and in very high demand. An orchestrated approach that allocates additional resources to the highest value targets is critically important. Spreading the cost of this work fairly across all global beneficiaries is essential to achieve sustainability and the LF is uniquely positioned to drive this global effort.

For CII, the first priority addressed OSS that was commonly adopted into enterprise infrastructure. We believe the next phase should focus on those OSS projects that are specifically used in security critical infrastructure use cases, such as energy and telecommunications.

The LF through CII, with the support of our partners IDA, LISH and Synopsys, intend to collectively pursue the next phase of identifying the critical OSS projects. Phase II of the CII effort will require resources, both financial and data, to better understand what OSS projects are critical to the security of our critical infrastructure.

This Committee in particular, through its thoughtful inquiry into the state of the OSS ecosystem, has an opportunity to support our efforts by encouraging industry to participate and provide access to data. Once the critical OSS projects are identified, the next step will require analyzing the projects and building an understanding of the community dynamics and processes which may present security risks. With this information industries will be enabled to invest in proactive-security and work with us to prevent security issues, such as Heartbleed, from arising in the future.

Software security will continue to be a global challenge due to the sheer volume of code being deployed in any modern system. OSS and closed source software share a susceptibility to defects that create opportunities for exploitation as a security vulnerability. Organizations dealing with security in a successful model invest and focus on deploying the software in a secure way and maintain processes of continuous security remediation. Heartbleed, the Equifax breach and many other similar incidents have proven that having a fix for software is not enough. Companies must know the contents of the software they are using and be able to identify any software component that has been determined to be vulnerable and ensure that all available patches and fixes to the software are deployed as soon as they are available and in all of the systems and devices affected. Because of how OSS is openly developed and deployed, there is a unique opportunity to collaborate on collective solutions to this problem.

The LF looks forward to the opportunity to work on this collective issue with industry leaders and academic partners to identify what response systems will help facilitate remediation of inevitable issues that arise, including implementing standards for identifying BOMs in software and establishing supply chain standards and processes. Finally, as the resources to identify, remediate and operationally secure infrastructure are scarce, there is ample opportunity for organizations interested in helping to collaborate on expanding the talent pool through incentives, training and education programs.

I welcome further discussion and collaboration on this important topic of national and global interest.

Sincerely,

James Zemlin
Executive Director
The Linux Foundation