CYBERSECURITY STRATEGY REPORT

Prepared by the Energy and Commerce Committee, Majority Staff

Table of Contents

I. Introduction

A. The Subcommittee's Cybersecurity Concepts and Priorities

In today's connected world, where nearly all devices—from the phones in our pockets, to the refrigerators in our kitchens, to the multi-million-dollar equipment that runs our electric grid—are linked together through the Internet, cybersecurity has at once become a household term and one of the most complicated, difficult issues facing society. Once a topic seen mostly as a nuisance, requiring the occasional password reset or new credit card, cybersecurity now regularly makes headlines as the Internet and connected technologies have become not only economic, diplomatic, and military tools, but integral parts of our daily lives. However, even as the Internet has rapidly developed to become a vital part of modern society, it appears that the integration of effective cybersecurity has not kept pace.

Recognizing this reality, the Oversight and Investigations Subcommittee has spent the past several years analyzing certain cybersecurity issues with impacts across the Energy and Commerce Committee's broad jurisdiction. Several patterns have emerged from the Subcommittee's work. Regardless of industry, size, or sophistication, the cybersecurity challenges organizations face are largely the same. Further, traditional information technology (IT) strategies seem largely ineffective at stemming the growing tide of cybersecurity incidents—which now range from ransomware attacks that can hold an entire company hostage to hackers' exploitation of a security vulnerability in the latest cellphone model.

These observations raise two important questions for the Subcommittee:

(1) What are the common, root-cause origins of cybersecurity incidents?

(2) If traditional IT strategies have proven ineffective, what *can* organizations do to better strengthen their cybersecurity capabilities?

With regard to the first question, through dozens of briefings, hearings, letters, reports, and roundtables, the Subcommittee identified six interrelated, core cybersecurity concepts that contribute to cybersecurity incidents:

Concept 1: There will always be unknown unknowns.

Concept 2: You can't protect what you don't know you have.

Concept 3: Software is no longer written, but assembled.

Concept 4: There must be a common cybersecurity language.

Concept 5: Digital assets age faster and less predictably than physical ones.

Concept 6: Cybersecurity takes a "whole-of-society" approach.

The identification of these principles shaped the Subcommittee's approach to cybersecurity and guided subsequent work. As each of these concepts emerged, the Subcommittee began exploring and analyzing possible strategies for addressing them. This effort allowed the Subcommittee to answer the second question, and culminated in six priorities:

Priority 1: The widespread adoption of coordinated disclosure programs.

Priority 2: The implementation of software bills of materials across connected technologies.

Priority 3: The support and stability of the open-source software ecosystem.

Priority 4: The health of the Common Vulnerabilities and Exposures (CVE) program.

Priority 5: The implementation of supported lifetimes strategies for technologies.

Priority 6: The strengthening of the public-private partnership model.

Identifying these priorities was not enough; over the past several years, the Subcommittee has produced individual products related to each of these priorities that address each of their associated core cybersecurity concepts:

B. The Subcommittee's Cybersecurity Work

The Oversight and Investigations Subcommittee's work on these topics began in earnest in 2013, following two major IT-related incidents within the Energy and Commerce Committee's jurisdiction: the data breach at Target that compromised nearly 110 million user records and the launch of healthcare.gov.[1] These issues, along with several other massive data breaches and high-profile cybersecurity incidents across several sectors within the Committee's jurisdiction—including in the automotive, medical, and commercial sectors—raised several questions about the efficiency and efficacy of IT and cybersecurity practices.[2] At the same time, complex legal issues were arising at the intersection of technology and the justice system, to which the Committee responded by participating in the Joint Encryption Working Group with the Committee on the Judiciary.[3] As this work continued, the Subcommittee began to hone in on the common concepts and priorities identified above, and began producing work related to each.

---

[1] Brian Krebs, *The Target Breach, By the Numbers*, KREBS ON SECURITY (May 6, 2014), https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/; Sean Gallagher, *The seven deadly sins of HealthCare.gov*, ARS TECHNICA (OCT. 29, 2013), https://arstechnica.com/information-technology/2013/10/the-seven-deadly-sins-of-healthcare-gov/.

[2] Taylor Armerding, *The 17 biggest data breaches of the 21st century*, CSO (Jan. 26, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html; Dan Goodin, *Newly discovered flaw undermines HTTPS connections for almost 1,000 sites*, ARS TECHNICA (Feb. 9, 2017), https://arstechnica.com/information-technology/2017/02/newly-discovered-flaw-undermines-https-connections-for-almost-1000-sites/; Andy Greeberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; *Hospital drug pumps are hackable, experts warn*, BBC (June 9, 2015), https://www.bbc.com/news/technology-33063345.

[3] *Encryption Working Group Year-End Report*, H. COMM. ON ENERGY & COMMERCE, H. COMM. ON THE JUDICIARY (Dec. 20, 2016), https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf.

1. Subcommittee Work Related to Coordinated Disclosure

The Oversight and Investigations Subcommittee's work on coordinated disclosure was prompted by both progress and controversy in the public and private sectors on the topic, including guidance for industry released by the Food and Drug Administration released in October 2014 regarding management of cybersecurity in medical devices and media reports regarding vulnerabilities in medical devices and automobiles.[4] In November 2015, the Subcommittee held a staff-level roundtable attended by private sector stakeholders to examine coordinated disclosure and its challenges and opportunities.[5] Focused specifically on coordinated disclosure within safety critical sectors like automotive and medical devices, it brought together experts to discuss how standard coordinated disclosure practices can or should be evolved to better address these sectors' equities and risks. Following a high-profile, non-coordinated disclosure involving a medical device in 2016, the Subcommittee held a second roundtable in February 2017 to encourage further engagement with and development of the topic.[6]

In January 2018, the Energy and Commerce Committee sent letters to seven information technology companies—Amazon, AMD, Apple, ARM, Google, Intel, and Microsoft—involved with the largest known coordinated vulnerability disclosure to date: the discovery and disclosure of cybersecurity vulnerabilities Spectre and Meltdown, which could enable the unauthorized disclosure of sensitive information relying on modern chipsets.[7] The letters commended the stakeholders' embrace of coordinated disclosure while also highlighting potential concerns and the need for continuous evolution and improvement. For example, the Committee was concerned that the information embargo imposed by some letter recipients may have disadvantaged other affected companies that needed to respond to both vulnerabilities. In addition, the Committee was concerned that critical infrastructure equities may not have been fully considered during the letter recipients' decisions regarding disclosure timelines due to the fact that critical infrastructure owners and operators must often test patches for weeks or months before implementation, rather than the hours or days provided during the Spectre and Meltdown disclosure. Each recipient of the letter provided a written response and a briefing to Committee

---

[4] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, THE FOOD & DRUG ADMIN. (Oct. 2, 2014), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf (FDA embrace of coordinated disclosure for medical devices); Charlie Osborne, *Hackers control medical pumps to administer fatal doses*, ZD NET (June 9, 2015), https://www.zdnet.com/article/hackers-can-control-medical-pumps-to-administer-fatal-doses/ (public disclosure of cybersecurity flaw after disagreement between researcher and company); Andy Greeberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; *Hospital drug pumps are hackable, experts warn*, BBC (June 9, 2015), https://www.bbc.com/news/technology-33063345 (hackers disable car engine driven by report on public highway).

[5] U.S. Committee on Energy & Commerce, Roundtable on Coordinated Disclosure, November 2015.

[6] Sean Gallagher, *Trading in stock of medical device paused after hackers team with short seller*, ARS TECHNICA (Aug. 26, 2016), https://arstechnica.com/information-technology/2016/08/trading-in-stock-of-medical-device-paused-after-hackers-team-with-short-seller/; U.S. Committee on Energy & Commerce, Roundtable on Coordinated Disclosure, February 2017.

[7] Letters from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. on Energy and Commerce, to Apple, Inc., Amazon, Advanced Micro Devices, Inc., ARM Holdings, PLC, Google, Inc., Intel Corp., and Microsoft Corp. (Jan. 24, 2018).

staff. The recipients acknowledged the Committee's concerns and provided additional insight and context into their decision-making processes, and pledged to continue working to improve coordinated vulnerability disclosure practices.

In July 2018, along with the Senate Committee on Commerce, Science, and Transportation, the Committee sent a letter to CERT Coordination Center following up on concerns raised about coordinated vulnerability disclosure (CVD) practices in the wake of Spectre and Meltdown.[8] The letter raised two potential gaps in the CVD process here based on the Committees' work involving this vulnerability: (1) whether the CVD process was adequately coordinated to ensure that companies, particularly those providing critical infrastructure, had enough time to test and implement patches prior to public disclosure of the vulnerabilities and that the U.S. government received timely notice of the CVD process; and (2) whether companies used precise terminology in describing the availability, not application, of patches. This latter distinction remains important with regard to patching issues, as a patch may be "available" without an affected user having "applied" it, which leaves the user unprotected. By using the two terms interchangeably, the Committees were concerned that organizations providing patches may have provided a false sense of security to users and the general public.

In October 2018, the Committee released a white paper entitled "The Criticality of Coordinated Disclosure in Modern Cybersecurity."[9] This white paper announced the Committee's support for coordinated vulnerability disclosure, explaining that such programs are a necessity for organizations in a society so heavily dependent on massively complex information systems and networks like the Internet and other connected technologies. It made two recommendations: that Congress clarify the legal environment in which coordinated vulnerability disclosures take place and that it find ways to support and encourage organizations to adopt such programs.

2. Subcommittee Work Related to Software Bill of Materials

In March 2017, an outbreak of the type of file-encrypting malware known as "ransomware" spread quickly across the globe, infecting hundreds of thousands of devices in dozens of countries in a matter of hours.[10] Dubbed "WannaCry," this strain of ransomware leveraged a powerful and widespread flaw in a popular computing operating system to spread quickly from device to device.[11] Most notably, the flaw was not a "zero-day," or unknown flaw, but one for which a patch had been available for months. However, many organizations were unaware of their exposure to the flaw due to the "black-box" nature of many medical technologies.

---

[8] Letter from the Hon. Greg Walden, H. Comm. on Energy & Commerce, and the Hon. John Thune, Sen. Comm. on Commerce, Science, & Transportation, to CERT/CC. (July 17, 2018).
[9] *The Criticality of Coordinated Disclosure in Modern Cybersecurity*, H. Comm. on Energy & Commerce (Oct 23, 2018), https://energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf.
[10] *See* Memorandum to Members, Subcommittee on Oversight and Investigations, Hearing on "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity," June 6, 2017, *available at* https://docs.house.gov/meetings/IF/IF02/20170608/106078/HHRG-115-IF02-20170608-SD011.pdf.
[11] *Id.*

WannaCry thus lent additional weight and urgency to a recommendation in a joint report from the public and private healthcare sectors, "Report on Improving Cybersecurity in the Health Care Industry", that was released in June 2017. The report made a series of recommendations for how the healthcare sector could better prepare for cybersecurity threats, including on software bill of materials, which directly addresses the type of challenge highlighted by WannaCry. The Task Force explained this recommendation, stating:

> Having a "bill of materials" is key for organizations to manage their assets because they must first understand what they have on their systems before determining whether these technologies are impacted by a given threat or vulnerability. Moreover, this transparency enables health care providers to assess the risk of medical devices on their networks, confirm components are assessed against the same cybersecurity baseline requirements as the medical device, and implement mitigation strategies when patches are not available.[12]

In response to the outbreak, report, and other related Subcommittee work, the Energy and Commerce Committee held a roundtable in August 2017 to discuss the opportunities and challenges presented by the recommendation to begin leveraging "bills of materials" in the healthcare sector.[13] Following that initial conversation, in November 2017, the Committee sent a letter to the Department of Health and Human Services (HHS) requesting that HHS convene an industry-wide process to find ways to develop, implement, and leverage software bill-of-materials (SBOM) across the health care sector.[14] In its response to the Committee, HHS set out their timetable to launch such a process:[15]

By July 30, 2018:	Announce the software BOM effort work stream to be conducted under the Healthcare Sector Coordinating Council (HSCC) MedTech Cyber Security Risk Management Task Group 1B.
By November 30, 2018:	Publish *Federal Register* notice for public meeting
By January 26, 2019:	Publish proposed agenda for public meeting
February 25, 2019:	Hold public meeting (draft deliverables will be vetted in a public setting)

[12] *Report on Improving Cybersecurity in the Health Care Industry*, HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, June 2017, https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.
[13] U.S. Committee on Energy & Commerce, Roundtable on Software Bills of Materials, August 2017.
[14] Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to the Hon. Eric D. Hargan, Deputy Secretary, Dept. of Health & Human Services (Nov. 16, 2017), https://energycommerce.house.gov/wp-content/uploads/2017/11/20171116HHS.pdf.
[15] Letter from Matthew D. Bassett, Assistant Secretary for Legislation, Dept. of Health & Human Services, to the Hon. Greg Walden, Hon. Frank Pallone, Jr., and Hon. Diana DeGette, H. Comm. on Energy & Commerce (Sept. 18, 2018), https://energycommerce.house.gov/wp-content/uploads/2018/09/091718-HHS-Reply-to-Chairman-Walden.pdf.

By August 24, 2019:	Publish meeting summary to include responses to any recommendations made at the meeting or in the docket for the meeting

3. Subcommittee Work Related to Open-Source Software

As modern information systems and products have continued to grow in scale, sophistication, and complexity, the Subcommittee's work recognized the critical importance that open-source software (OSS) plays. The Energy and Commerce Committee sent a letter in April 2018 to the Linux Foundation, which leads an organization dedicated to the health and stability of OSS, requesting additional information on how OSS may be better supported.[16] The letter acknowledged that OSS has become "critical cyber infrastructure" and that, consequently, "the sustainability and stability of the OSS ecosystem is essential to the sustainability and stability of organizations' cybersecurity generally."[17]

The Linux Foundation responded on April 23, 2018, agreeing with the Committee's assessment and stating "it is the 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" and "[i]t 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."[18]

4. Subcommittee Work Related to the Common Vulnerabilities and Exposures Program

While cybersecurity strategies, policies, and procedures remain largely individualized from organization to organization, there exist some foundational cornerstones that all such programs require. One of those cornerstones is the Common Vulnerabilities and Exposures (CVE) program, the standardized naming scheme for cybersecurity vulnerabilities the world over. In 2016, public reports emerged that the CVE program was struggling to fulfill its purpose and meet stakeholder needs.[19]

In response, beginning in March 2017 and culminating in August 2018, the Energy and Commerce Committee investigated the health and stability of the CVE program. In March 2017, the Committee requested documentation from the program's responsible organizations, DHS and

---

[16] Letter to Mr. Jim Zemlin, Executive Director, the Linux Foundation, from the Hon. Greg Walden and Hon. Gregg Harper, H. Comm. on Energy and Commerce (Apr. 2, 2018), https://energycommerce.house.gov/wp-content/uploads/2018/04/040218-Linux-Evaluation-of-OSS-Ecosystem.pdf.

[17] *Id.*

[18] *Id.*

[19] Catalin Cimpanu, *CVE System Sees Huge Backlog, Researchers Propose Alternative*, SOFTPEDIA, Mar. 12, 2016, http://news.softpedia.com/news/cve-system-sees-huge-backlog-researchers-propose-alternative-501665.shtml; Sean Sposito, *CVE, a key cybersecurity resource, is at risk inside and out*, SAN FRANCISCO CHRONICLE, Mar. 25, 2016, http://www.sfchronicle.com/business/article/CVE-a-key-cybersecurity-resource-is-at-risk-7107509.php; CSO, *Over 6,000 vulnerabilities went unassigned by MITRE's CVE project in 2015,* CSO ONLINE, Sep. 22, 2016, http://www.csoonline.com/article/3122460/techology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.html.

MITRE, including all contracts associated with the CVE program and any timelines, analyses, or other relevant documentation detailing the oversight both organizations had performed throughout the program's lifetime.[20]

In August 2018, the Committee sent a second letter to DHS and MITRE summarizing the findings of the investigation, including that the contract vehicle for the CVE program was awarded or modified 30 times in nearly seven years, that funding for the program varied acutely, and that neither DHS nor MITRE conducted substantial oversight of the program.[21] The second letter made recommendations to both organizations based on the produced documentation, mainly that DHS should transition the CVE program to a dedicated Program, Project, or Activity funding model, and that DHS and MITRE should perform biennial reviews of the CVE program to ensure its effectiveness and stability.[22]

In September 2018, the Cyber Threat Alliance and the Cybersecurity Coalition, two groups comprised of cybersecurity companies and experts dedicated to advancing and improving robust cybersecurity practices and policies, expressed agreement with the recommendations made to DHS and MITRE. In a letter to the Committee, the groups wrote, "The Committee's August 27th letters noted the CVE program's importance, referring to it as 'critical cyber infrastructure.' We concur with the Committee's assessment."[23]

5. Subcommittee Work Related to Supported Lifetimes

The ransomware outbreak known as WannaCry, followed closely by an outbreak of an even more destructive strain of malware known as NotPetya, highlighted the cybersecurity risks that the use of old, outdated technologies pose. In recognition of both that fact, and that addressing such risks is a complex, multi-faceted problem, the Committee on Energy and Commerce in April 2018 released a Request for Information (RFI) seeking input on how to address legacy technology and related issues in the health care sector. The RFI stated that "[t]he challenges created by legacy technologies are, by definition, decades in the making. They implicate dozens of diverse stakeholders with different and at times competing equities, and they have no clear solutions . . . [t]o understand the full scope of the challenge and potential paths to

[20] Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to Mr. Jason Providakes, President and Chief Executive Officer, MITRE Corp. (March 31, 2017); Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to the Hon. General John F. Kelly, Sec'y, U.S. Dep't of Homeland Security (March 31, 2017).

[21] Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to Mr. Jason Providakes, President and Chief Executive Officer, MITRE Corp. (Aug. 27, 2018); Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to the Hon. Kristjen Nielsen, Sec'y, U.S. Dep't of Homeland Security (Aug. 27, 2018).

[22] *Id.*

[23] Letter from Cybersecurity Coalition and Cyber Threat Alliance to Hon. Greg Walden, Hon. Gregg Harper, Hon. Marsha Blackburn, and Hon. Robert E. Latta (Sept. 11, 2018), https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/Joint-Coalition-CTA-Letter-to-House-EC-on-CVE-9112018.pdf.

address it, [the Committee requires] insight from stakeholders of all sizes, from all parts of the health care sector."[24]

In response, the Committee received nearly 300 pages worth of comments. For example, many stakeholders agreed with two of the Committee's existing priorities, coordinated vulnerability disclosure and software bill of materials, while raising many additional complex issues to be considered. Following the RFI's release and the receipt of comments, the Committee continues to explore supported lifetimes challenges and opportunities, including a staff-level roundtable in October 2018 with members of the healthcare sector to discuss how to improve transparency and clarity with regards to legacy technology risks, roles and responsibilities, and strategies.[25]

6. Subcommittee Work Related to The Public-Private Partnership Model

While the nation is experienced at responding to threats to critical infrastructure from natural and man-made disasters, both the public and private sectors continue to explore and evolve their strategies for addressing cybersecurity threats. Throughout the first half of 2017, the Subcommittee on Oversight and Investigations held several events focused on the public-private partnership model established under current law that provides a framework for responding critical infrastructure threats caused by cybersecurity incidents.

At the first event, a roundtable discussion, Committee Members and representatives from public-private partnership organizations discussed current challenges and opportunities. On April 4, 2017, the Subcommittee held a hearing entitled "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships" at which members heard testimony from Denise Anderson, President, National Health Information Sharing and Analysis Center, Michael McNeil, Global Product Security and Services Officer, Phillips, and Terry Rice, Vice President, IT Risk Management and Chief Information Security Officer, Merck & Company, Inc. At that hearing, both Members and the witnesses focused on the fact that modern heath care cybersecurity is no longer just about protecting patient data or information, but that it has become a patient safety issue.[26]

On June 8, 2017, the Subcommittee held a hearing entitled "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity" at which members heard testimony from Emery Csulak, Chief Information Security Officer and Senior Privacy Official, Centers for Medicare and Medicaid Services and co-chair, Health Care Industry Cybersecurity Task Force, Steve Curren, Director, Division of Resilience, Office of Emergency Management, Office of the Assistant Secretary for Preparedness and Response, and Leo Scanlon, Deputy Chief Information Security Officer, U.S. Department of Health and Human Services. At

---

[24] *Supported Lifetimes Request for Information*, H. Comm. on Energy & Commerce (Apr. 20, 2018), https://energycommerce.house.gov/wp-content/uploads/2018/04/20180420Supported_Lifetimes_RFI.pdf.
[25] U.S. Committee on Energy & Commerce, Roundtable on Supported Lifetimes, October 2018.
[26] *Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships Before the Subcomm. On Oversight & Investigations*, 115th Cong. (Apr. 4, 2017), https://energycommerce.house.gov/hearings/cybersecurity-heath-care-sector-strengthening-public-private/.

this hearing, which took place only weeks after the WannaCry infection that crippled health care systems in the United Kingdom, members highlighted the criticality of the Department's role as a leader and partner in health care cybersecurity and pressed the witnesses to ensure that Department remained effective at both.[27]

* * *

This report seeks to combine the work described above into an overarching strategy detailing why the Subcommittee selected these core concepts, why these priorities represent the most effective strategies for addressing them, and, most importantly, why each concept and each priority is inextricably linked to its fellows.

Cybersecurity's importance grows in parallel to society's dependence on the Internet and connected technologies. Over the course of the last two decades, the Internet has exponentially expanded and society's dependence on connected technologies has exploded. If the growth during that period is to serve as a guide, cybersecurity is and will continue to be one of the premier issues facing governments, companies, and individuals globally. This report represents the culmination of the Subcommittee's initial efforts illuminate these issues for use by the full Committee on Energy and Commerce, and to assist with its various and ongoing legislative work addressing cybersecurity matters across its jurisdiction.

[27] *Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity Before the Subcomm. On Oversight & Investigations*, 115th Cong. (June 8, 2017), https://energycommerce.house.gov/hearings/cybersecurity-heath-care-sector-strengthening-public-private/.

II. Coordinated Disclosure: Because There Will Always Be Unknown Unknowns

A. Concept: There Will Always Be Unknown Unknowns

As the Subcommittee on Oversight and Investigations led Committee efforts to investigate the growing number of cybersecurity incidents over the past several years, a common trend emerged: organizations that suffer cybersecurity incidents often do not discover those incidents themselves. Federal agents notified 3,000 companies in 2013 that they had suffered data breaches.[28] Two independent security researchers discovered the infamous "Jeep hack" found to affect certain Chrysler vehicles.[29] Google, Intel, Johnson & Johnson, General Motors, and even the United States Department of Defense have each been informed of cybersecurity vulnerabilities in their systems by external parties.[30] At first glance, the fact that organizations are not discovering their own incidents may seem irresponsible. But in looking at the complexity of modern systems, it is clear why this is the case.

Modern information systems and networks contain hundreds to thousands of individual hardware and software components, each of which typically contain dozens of software libraries and thousands of lines of code, which in turn may be vulnerable to various cybersecurity flaws or risks. The exact combination of these components then varies from network to network, where organizational requirements or misconfigurations may introduce new sources of vulnerability. Exacerbating the situation, one organization's network is then connected to additional networks, and in doing so inherits the complexity and vulnerabilities of each system to which it is attached. As frustrating as it seems, in cybersecurity, there will always be "unknown unknowns."

The recognition of this fact gives rise to a daunting question—what can an organization do about it? It is unacceptable to take no action, since the frequency and severity of cybersecurity incidents has been increasing steadily and shows no signs of slowing. Expecting organizations to identify all their unknown unknowns, however, would be impractical and counterproductive. One way to solve this problem, which has been implemented in many modern cybersecurity incidents, is third-party disclosure. To put it simply, even if an organization doesn't know what it doesn't know, someone else might. And better yet—that entity might be willing to work with the affected organization to fix it.

---

[28] Ellen Nakashima, *U.S. notified 3,000 companies in 2013 about cyberattacks*, WASH. POST (Mar. 24, 2014), https://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html?utm_term=.e8e60d8f5dd1.

[29] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me In It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[30] Lisa Ferdinando, *Carter Announces 'Hack the Pentagon' Program Results*, U.S. DEPT. OF DEFENSE (June 17, 2016), https://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/; Tod Beardsley, *R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump*, RAPID7 (Oct. 4, 2016), https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/; Peter Bright, *Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it,* ARS TECHNICA (Jan. 5, 2018), https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/; Kate Conger, *General Motors is Expanding Its Bug Bounty Program*, GIZMODO (Mar. 15, 2018), https://gizmodo.com/general-motors-is-expanding-its-bug-bounty-program-1823809720.

B. Priority: Coordinated Disclosure

Coordinated disclosure is a collaborative vulnerability identification and remediation process. A coordinated disclosure occurs when a "finder," whose identity can range from an independent individual to a large, multi-billion-dollar company, discovers a cybersecurity vulnerability or incident and then notifies the "owner" of the affected product or network about the issue. These parties then typically work together behind the scenes to validate the findings, develop a patch or mitigation, and then publicly announce both the flaw and the fix at an agreed-upon time. While coordinated disclosures can and do occur on an ad-hoc basis, the most successful coordinated disclosures generally take place within official coordinated disclosure programs adopted by organizations.

An organization's adoption of a coordinated disclosure program produces numerous benefits. It allows an owner to invite the aid and expertise of outside parties in identifying an organization's unknown unknowns, potentially avoiding a cybersecurity incident later, while setting "ground rules" for third-party investigations of its data and networks. This scoping helps to avoid unintended consequences such as outages or data destruction, and allows an owner to simultaneously protect its assets and customers while receiving the full benefits of coordinated disclosure. Finders in turn benefit through the ability to perform cybersecurity research without fear of civil or criminal penalties, incentivizing them to ferret out otherwise invisible bugs and report them to the affected owner. By enabling both behaviors, coordinated disclosure programs facilitate the protection of society at large by providing robust mechanisms through which cybersecurity vulnerabilities may be found and fixed before they become a widespread threat.

The existence of coordinated disclosure recognizes the reality that all organizations will always have cybersecurity unknown unknowns. But organizations' accelerating adoption of coordinated disclosure programs serves as an acknowledgement that one of the most effective ways to address those unknowns is to invite collaboration and cooperation. Such programs greatly increase the chance that an organization will be made aware of potential vulnerabilities before they lead to a cybersecurity incident that negatively impacts the organization, its partners, and users. Coordinated disclosure is, however, only the first step in addressing the myriad cybersecurity threats facing organizations and society. The next step is to minimize as many of those unknown unknowns as possible.

Committee Products: Roundtables and Spectre and Meltdown Investigation

In November 2015 and February 2017, the Energy and Commerce Committee held staff-level roundtables with private sector stakeholders to examine coordinated disclosure and its challenges and opportunities.

In January 2018, the Energy and Commerce Committee sent letters to stakeholders responsible for the largest known coordinated vulnerability disclosure to date.

In July 2018, the Energy and Commerce Committee and the Senate Committee on Commerce, Science, and Transportation sent a follow-up letter to CERT/CC asking them to incorporating lessons learned from recent coordinated disclosures.

In October 2018, the Energy and Commerce Committee released a white paper, "The Criticality of Coordinated Disclosure in Modern Cybersecurity."

III. Software Bill of Materials: Because You Can't Protect What You Don't Know You Have

A. Concept: You Can't Protect What You Don't Know You Have

Two major incidents in recent years have underscored the stark truth that, in cybersecurity, you can't protect what you don't know you have: the discovery of the critical vulnerability known as Heartbleed and the outbreak of the widely infectious ransomware known as WannaCry. Amid both incidents, organizations looking to protect themselves scrambled to find out if they were vulnerable. This arguably straightforward inquiry turned into a Pandora's box, however, as organizations quickly realized that, due to incomplete asset and inventory lists of the technologies in their environments, they didn't know if their systems and networks were exposed to either threat. This in turn led to an even more problematic realization: even if they *had* perfect inventory lists, the black-box nature of many technologies would stymie their efforts.

Heartbleed and WannaCry took place three years apart, the former in 2014 and the latter in 2017. Regardless, organizations found themselves facing the same challenge. Due to the black-box nature of most technologies, organizations did not know, and had no straightforward way to discover, what hardware or software they were running. This lack of visibility—which still exists today, across all sectors and many technologies—forces organizations to try to mitigate cybersecurity vulnerabilities blindly, relying on sporadic and usually opaque vendor guidance when it's provided, or on broad-stroke best practices when it's not. By demonstrating the consequences that can arise when organizations lack visibility into the technologies in their environments, Heartbleed and WannaCry provided two painful examples of the following concept—you can't protect what you don't know you have.

As *some* unknown unknowns are inevitable, the most effective method for organizations to address this reality is to maximize what they know. As illustrated by Heartbleed and WannaCry, organizations need to dramatically improve their asset and inventory strategies to ensure that these lists are comprehensive and up-to-date. As Heartbleed and WannaCry also revealed, however, this is not enough. Organizations must find some way to crack open the current technology black boxes that they are connecting to their systems so that they may fully assess their risks and, as a result, more completely understand their organization's cybersecurity exposure.

B. Priority: Software Bill of Materials

One way for an organization to be better prepared to respond to vulnerabilities is to have a software bill of materials (SBOM) that details the components that form the technology it uses. The concept has existed for many years in various forms, but a 2017 report included the practice as an official recommendation for government agencies.[31] In short, SBOM becomes an ingredients list for a given piece of technology, listing the hardware, software, and other relevant components that it contains or relies upon. This creates two primary benefits. First, it permits organizations to make informed risk decisions about which technologies to purchase and use based on known

[31] *Report on Improving Cybersecurity in the Health Care Industry*, HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, June 2017, https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.

vulnerability information. Second, when new vulnerabilities are discovered, it allows organizations to quickly identify their exposure and to take appropriate steps in response.

The problem highlighted by Heartbleed and WannaCry was not that organizations did not know which software was vulnerable—that information was made publicly available from the outset—it was that they did not know which pieces of technology that *they depended on* included it. SBOM addresses this issue by cracking open otherwise black box technologies. In doing so, it helps minimize the number of unknown unknowns with which organizations must contend, and greatly increases their ability to protect themselves, their users, and ultimately society, by giving them much-needed cybersecurity data to which they can respond.

Much like coordinated disclosure, however, SBOM is not an end in and of itself. Once organizations have access to and have developed methods to leverage SBOM and minimize their unknown unknowns, these ingredient lists by their nature will reveal additional factors. One of the primary factors that any SBOM will quickly make clear is that, in addition to the proprietary technologies that organizations know that they are acquiring when they purchase IT, organizations will see the pervasiveness of open-source software—which they often do not know they're acquiring.

Committee Product: Software Bill of Materials Letter

In August 2017, the Energy and Commerce Committee convened a staff-level roundtable with members of the healthcare sector to discuss the opportunities and challenges associated with SBOM design and deployment.

Following that initial discussion, in November 2017, the Energy and Commerce Committee sent a letter to the Department of Health and Human Services (HHS) requesting that HHS convene an industry-wide process to find ways to develop, implement, and leverage SBOM across the health care sector. In response, HHS launched this process in 2018, which will conclude in 2019.

IV. Supporting Open-Source Software: Because Software Is No Longer Written, But Assembled

A. Concept: Software is No Longer Written, But Assembled

Walk into nearly any office in today's connected world, and it is likely that the desks will be topped by computers running Microsoft's Windows or Apple's macOS. Their screens might show websites open in Google's Chrome or Microsoft's Edge, and smartphones running Apple's iOS or Google's Android will likely be sitting next to keyboards. The ubiquity of such proprietary technologies is so well-known that it is taken for granted. What remains less well-understood are the technologies and software running under the hood of each of those products. The Windows operating system is not constructed solely of Microsoft-developed code.[32] Android phones and iPhones contain more than Google- or Apple-designed software.[33] Today, an organization's technology rarely consists solely of that organization's code.

For the same reasons that physical manufacturing moved away from bespoke craftmanship to assembly-line-based manufacturing, software development has moved from an artisanal, soup-to-nuts process to one more akin to bricklaying. The bricks are supplied by open-source software (OSS), which provides free, customizable code packages that typically perform one programming task—such as data encryption or storage—reliably and efficiently. Like screws, nuts, or washers, whose standardized characteristics allow their use across an array of physical products and whose availability eliminates the need for companies to develop custom tools, OSS may be built into larger pieces of software to take care of common programming staples. The benefits of doing so are so remarkable, in fact, that one study estimates that 78 percent of companies "run on OSS."[34] Consequently, software is no longer written, but assembled.

With that concept comes a corollary; in such a world, the quality of the bricks used to assemble software becomes critically important. If 78 percent of companies rely on OSS, then OSS vulnerabilities—reliability, cybersecurity, or otherwise—can pose an immediate and widespread threat to a significant portion of modern organizations. Considering that many pieces of OSS are developed and maintained by globally-located volunteers, many of whom are unpaid and have unrelated full-time employment, it is no longer enough for organizations to prepare for Microsoft's infamous Patch Tuesdays, or for IT departments to ensure that their workforces are running the latest iOS on company iPhones. Now, these organizations must recognize the critical importance of OSS and behave accordingly.

---

[32] *Open Source at Microsoft*, MICROSOFT (last visited Apr. 11, 2018), https://opensource.microsoft.com/.
[33] *Open Source*, APPLE (last visited Apr. 11, 2018), https://developer.apple.com/opensource/; *Google Open Source*, GOOGLE (last visited Apr. 11, 2018), https://opensource.google.com/projects/list/featured.
[34] *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.

B. Priority: Supporting Open-Source Software

Stakeholder support for OSS is neither a particularly new nor complicated policy proposition. The Heartbleed vulnerability—before it became a key exhibit in the argument for better technology transparency and SBOM—led many organizations to recognize their status as OSS-reliant stakeholders, and prompted the very behavior changes the pervasiveness of OSS requires. While examples like the Core Infrastructure Initiative remain the clearest manifestations of these changes, as the Initiative's members include some of the largest technology companies in the world and it provides funding and other support for the OSS ecosystem, it is not the only example.[35] Some organizations now allow and encourage their programmers to contribute to OSS as part of their duties, and others have "open-sourced" some of their own code to better promote software quality across the connected ecosystem.[36]

Each of these contributions, whether on the global scale of the Initiative or the smaller scale of individual company efforts, helps improve the overall health of the OSS ecosystem. They recognize that OSS is not just another shared resource; OSS components form such a substantial part of the Internet's foundation that to strengthen one is to strengthen the other. As a result, such contributions enable some of the highest return-on-investment for companies looking to improve cybersecurity for a relatively low cost. After all, if 78 percent of companies run on OSS, then any improvement in the quality of OSS bricks will create immediate, widespread, and effective increases in the overall quality of the cybersecurity capabilities of the organizations using them.

OSS support, together with coordinated disclosure and SBOM, recognize and address some of the most critical facets of organizations' modern cybersecurity challenges. The combination of these three priorities allows organizations to simultaneously accept their unknown unknowns, minimize as many of them as possible, and support the quality of the shared software resources upon which they, their partners, and their customers rely. At some point, however, organizations need to look outside of themselves to truly understand their cybersecurity exposure and manage their cybersecurity risks. When that occurs, organizations need a common cybersecurity language.

Committee Product: Open-Source Software Letter

In April 2018, the Energy and Commerce Committee sent a letter to the Linux Foundation, which leads the Core Infrastructure Initiative, requesting additional information on how OSS may be better supported. The Committee continues to analyze the response and explore ways to ensure the stability and effectiveness of the OSS ecosystem.

[35] *FAQ – What is the Core Infrastructure Initiative?*, CORE INFRASTRUCTURE INITIATIVE (last visited Jan. 17, 2018), https://www.coreinfrastructure.org/faq.
[36] Cynthia Harvey, *35 Top Open Source Companies*, DATAMATION (Sep. 21, 2017), https://www.datamation.com/open-source/35-top-open-source-companies-1.html.

V. The CVE Program: Because There Must Be a Common Cybersecurity Language

A. Concept: There Must Be a Common Cybersecurity Language

Setting aside clever marketing names like Meltdown, FREAK, or Heartbleed, when cybersecurity vulnerabilities are found today, they are not identified by a description of the vulnerability itself—which may be, in strict terms, several flaws chained together—but by a Common Vulnerabilities and Exposures Identifier or CVE ID. Overseen by the Department of Homeland Security (DHS) and maintained by federal contractor MITRE, the CVE program has provided unique identifiers for over 100,000 vulnerabilities during its two decades in existence.[37] In a world where cybersecurity incidents can occur in a fraction of a second, with flaws that range from straightforward to outright labyrinthine, the ability enabled by the CVE program to instantaneously identify a vulnerability is critical to modern cybersecurity professionals, products, and practices.

This fact was made abundantly clear in the spring of 2016, when multiple media outlets reported that the CVE program was struggling to keep up with the number of vulnerabilities reported.[38] As the program administrators later publicly admitted, the explosive growth of connected technologies had caught the program off-guard.[39] Consequently, ID assignments were delayed for weeks or sometimes months, and some vulnerabilities were deemed "out of scope" for the program and rejected outright.[40] As outlined in the press reports, these issues had immediate, noticeable impacts on the cybersecurity industry.[41] It was during this period, as stakeholders caught a glimpse of what a world without CVE might look like, that the following concept became clear: there must be a common cybersecurity language.

What also became exceedingly clear is that the CVE program already is that common language. Over its two decades, the CVE program has become more than just another convenient government service; it is the cornerstone on top of which modern cybersecurity is constructed. It took the 2016 press reports to shine a light on not just this truth, but on the far more uncomfortable truth that CVE stakeholders, both in the public and private sector, had taken the program for granted. To protect the CVE program, the root-causes of problems affecting the program needed identification and remediation.

---

[37] *About CVE*, THE MITRE CORPORATION (last visited Nov. 30, 2018), https://cve.mitre.org/about/.
[38] Catalin Cimpanu, *CVE System Sees Huge Backlog, Researchers Propose Alternative*, SOFTPEDIA, Mar. 12, 2016, http://news.softpedia.com/news/cve-system-sees-huge-backlog-researchers-propose-alternative-501665.shtml; Sean Sposito, *CVE, a key cybersecurity resource, is at risk inside and out*, SAN FRANCISCO CHRONICLE, Mar. 25, 2016, http://www.sfchronicle.com/business/article/CVE-a-key-cybersecurity-resource-is-at-risk-7107509.php; CSO, *Over 6,000 vulnerabilities went unassigned by MITRE's CVE project in 2015,* CSO ONLINE, Sep. 22, 2016, http://www.csoonline.com/article/3122460/techology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.html.
[39] *News & Events – FOCUS ON: CVE Program Status*, THE MITRE CORPORATION, Mar. 21, 2016, https://cve.mitre.org/news/archives/2016/news.html#march212016_FOCUS_ON_CVE_Program_Status_Update.
[40] *See supra* note 11.
[41] *See supra* note 11.

B. Priority: The CVE Program

The Committee on Energy and Commerce opened an investigation into the CVE program in March 2017.[42] That investigation acknowledged that while steps had been taken to improve the program's effectiveness and stability following the 2016 press reports, neither DHS nor MITRE had provided an explanation as to *how* the program had become so unprepared. To answer that question and ensure that the same or similar issues would not reoccur, the Committee requested and reviewed contract and management documentation related to the CVE program. That review found that instability in the program's funding and management mechanisms were primarily at fault, and resulted in two recommendations: that DHS move the CVE program from a contract-based funding model to a dedicated Program, Project, or Activity and that both DHS and MITRE should perform biennial reviews of the program. The Committee believed these recommendations would strengthen the program and minimize the likelihood of serious problems once again interfering with its operation.

Both the Committee's investigation and its recommendations acknowledge that the CVE program is the foundation upon which modern cybersecurity practices are built and the common language that modern cybersecurity practitioners speak. By exercising its authority to analyze the historical factors that had allowed the CVE program's problems to manifest and grow entrenched, and then shaping the resulting conclusions into actionable recommendations, the Committee sought to ensure that a critical cybersecurity resource did not collapse. More than that, the recommendations were targeted at creating an environment in which the CVE program would be able to grow and evolve in parallel to the very stakeholders it is meant to serve.

The CVE program, like coordinated disclosure, SBOM, and OSS support, remains another critical cybersecurity building block. To be truly effective, organizations must continue building atop it, and leverage the common cybersecurity language it creates to better understand and analyze their IT and cybersecurity posture. In doing so, organizations using the program and its vocabulary of CVE IDs will quickly be confronted with the fact that all digital technologies are vulnerable and the older a technology is, the more vulnerable it becomes.

Committee Products: Oversight Letters on the CVE Program (March 2017, August 2018)

Beginning in March 2017 and culminating in August 2018, the Energy and Commerce Committee investigated the health and stability of the CVE program. The first letter requested documentation from the program's responsible organizations, DHS and MITRE, while the second made recommendations to both organizations based on the produced documentation.

[42] Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to Mr. Jason Providakes, President and Chief Executive Officer, MITRE Corp. (March 31, 2017); Letter from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to the Hon. General John F. Kelly, Sec'y, U.S. Dep't of Homeland Security (March 31, 2017).

VI. Supported Lifetimes: Because Digital Assets Age Faster and Less Predictably Than Physical Ones

A. Concept: Digital Assets Age Faster and Less Predictably Than Physical Ones

While recent newsworthy cybersecurity incidents have targeted a wide variety of victims and varied wildly in sophistication, effectiveness, and consequences, many share a common factor: the exploitation of old or legacy technologies. The infamous WannaCry outbreak that ravaged the healthcare sector exploited a 30-year-old protocol.[43] Triton, a strain of malware designed to target industrial control systems within the energy sector, relied upon a vulnerability in a legacy version of a manufacturer's firmware.[44] More generally, many malware authors leverage "exploit kits," which combine multiple known vulnerabilities into a single package that, upon execution by unsuspecting victims, attempt to exploit any unpatched, legacy software or firmware on a victim's device.[45]

This trend is borne out in more than just anecdotal data; a cursory examination of any technology's CVE IDs shows that the number of associated discovered vulnerabilities increases over time. Like physical products later found to have some flaw under certain circumstances, the very process of putting digital technologies into use will stress them and reveal both reliability and cybersecurity issues. Further exacerbating this is the pace of technological innovation; organizations are constantly developing or searching for new, more advanced technologies to better carry out their missions. As a result, legacy technologies receive less support and attention as time goes on. This confluence of factors leads to the following concept; digital assets age faster and less predictably than physical ones.

When faced with the potentially severe consequences created by this concept, a seemingly ideal and obvious solution presents itself; decommission the technologies. After all, doing so would completely eliminate the threat of their exploitation, and often whatever new technologies replace older versions will include additional advanced features that benefit the organization in addition to reducing risk. But that recommendation ignores the complicated and controversial context in which legacy technologies exist. The problems created by legacy technologies are, by definition, decades in the making. Their solutions are unlikely to be less so.

B. Priority: Supported Lifetimes

The first step in examining the legacy technologies problem is to realize that the issue extends far beyond the technologies themselves. The risks associated with the use of legacy technologies raise numerous questions. How long should organizations that develop or maintain technologies be required to support them? How long should organizations that use those

---

[43] Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED, Mar. 12, 2017, https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

[44] *Important Security Notification – Malware Discovered Affecting Triconex Safety Controllers V2.0*, SCHNEIDER ELECTRIC (Jan. 18, 2018), https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Id=9555022209&p_File_Name=SEVD-2017-347-01+Triconex+V2.pdf&p_Reference=SEVD-2017-347-01.

[45] Joshua Cannell, *Tools of the Trade: Exploit Kits*, MALWAREBYTES (Oct. 17, 2016), https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/.

technologies be permitted to reasonably rely on them? Some technologies continue to exhibit perfectly acceptable physical function long after their digital components age—must they still be replaced in their entirety? With this context, referring to these issues as the "legacy technology problem" is reductive and misleading. Instead, the Committee groups these issues under the heading "Supported Lifetimes" and examines them holistically.

If legacy technologies and their associated, intractable Supported Lifetimes questions are to be addressed, the solutions will require creativity, cooperation, and compromise. Technology developers will likely need to provide some guaranteed minimum support lifetime to the products they sell. Users will have to accept and plan for the phasing out of technologies as they get older, whether or not their physical performance is optimal. Beyond that, technology development strategies will likely need to be carefully reexamined. Is it possible, for example, to decouple physical assets from digital ones, so that the obsolescence of one does not necessarily force the obsolescence of the other? Should organizations move to a technology-leasing model, rather than a purchasing model, so that manufacturers may swap old, vulnerable technologies with new, more secure ones with greater ease? These types of Supported Lifetimes questions and more require careful but prompt consideration.

A common thread running through each of the five concepts already discussed is that all require collaboration between diverse and at times competing stakeholders whose technologies and networks are all inextricably linked. An organization on its own may be able to protect a single computer running isolated code, unplugged from the Internet or any other devices, but that computer is unlikely to be particularly useful. The power of connected technologies is just that – connection. By necessity, then, protecting these technologies requires protecting each end of the connection. And that will require partnership.

Committee Product: Supported Lifetimes Request for Information

In April 2018, the Committee on Energy and Commerce released a Request for Information seeking input on how to address legacy technology and related issues in the health care sector. The Committee continues to review the received responses and plans to pursue initiatives based on stakeholder perspectives and feedback.

As part of the Committee's review and continued exploration of RFI responses, the Committee held a staff-level roundtable in October 2018 with stakeholders to discuss how to improve transparency and clarity with regards to legacy technology risks, roles and responsibilities, and strategies.

VII. The Public-Private Partnership Model: Because Cybersecurity Requires a "Whole-of-Society" Approach

A. Concept: Cybersecurity Requires a "Whole-of-Society" Approach

With news of cybersecurity incidents dominating headlines on a regular basis, government agencies, private companies, and individual users have become aware of the cyber threat. Government agencies are required by law to meet certain cybersecurity standards. Organizations are constantly seeking new, innovative solutions to protect their systems and secrets from prying digital eyes. Even consumers now seek out cybersecurity guides for advice on how best to protect themselves from identity thieves, ransomware, fake apps, and more. Too often, though, each of these groups try to manage cybersecurity risks and protect themselves from cyber threats on their own. This is a strategy doomed to fail. True cybersecurity, in this case, takes at least two. And on the Internet, it takes a great many more than that.

Cybersecurity is a shared problem, and not just abstractly. The Internet by its technical design requires at least two devices, connected through wires or spectrum, communicating through standardized networking protocols. Consequently, even if one end of a connection is secure, the other might not be, and that puts both at risk. Multiplied by the millions upon millions of individual connections that make up the Internet, the end result is that the only feasible way to provide any appreciable level of cybersecurity is cooperation. More so than nearly any other shared resource, cybersecurity requires a "whole-of-society" approach, in which individuals and organizations across both the public and private sectors play vital, integral roles.

This reality becomes even more complicated when the composition of the modern Internet is taken into full consideration. At its inception, the Internet was made up primarily of consumer devices like personal computers, servers, and other business-centric devices. Now, it includes smart grid equipment, medical devices, connected cars, critical manufacturing equipment, and much more. Today, diplomatic and military secrets transit the same networks as social media posts and viral videos. Exacerbating the situation further, many of these connected critical infrastructure components are owned and operated by the private sector, which makes public-private partnership in cybersecurity more than just a catchphrase, but essential; without it, many cybersecurity strategies fail altogether.

B. Priority: The Public-Private Partnership Model

In the United States, a Public-Private Partnership model has been established for designated critical infrastructure through Presidential Policy Directive 21 ("PPD-21") and its predecessors.[46] These policies divide critical infrastructure into 16 sectors and assign several roles and responsibilities to public and private sector representatives within each. Three of the most critical roles designated in PPD-21 are: Sector-Specific Agencies (SSAs), responsible for overseeing and guiding their sectors; Sector Coordinating Councils (SCCs), voluntary groups consisting of private sector representatives who work with and represent industry equities to their SSAs; and

[46] *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, THE WHITE HOUSE (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Information Sharing and Analysis Centers (ISACs), official public-private forums for the sharing of information between sector members.

While these roles and acronyms may seem academic, their criticality—especially in cybersecurity—is undeniable. The hybrid nature of the Internet, where data and information critical to national and economic security flow over and through cables, networks, and devices owned and operated by the private sector, requires cooperation on a level that would likely be impossible to achieve without a framework like the one created by PPD-21. Further, while the sophistication of the different sectors varies significantly, the sectors with the strongest SSAs, SCCs, and ISACs are almost universally considered to be the gold standard with regards to cybersecurity capabilities and readiness. Considering that critical infrastructure sectors include those like energy, telecommunications, and information technology—the sectors, in other words, the make the Internet possible—the strengthening of these 16 sectors and the PPD-21 public-private partnership model strengthens the Internet as a whole.

The public-private partnership model is the sixth and final priority identified by the Subcommittee through its cybersecurity work. It builds on and incorporates each of the priorities examined before it, as, after all, the information shared through this model no doubt includes vulnerabilities discovered through coordinated disclosure, context derived from SBOM, details around OSS usage, and supported lifetimes risks and strategies, all shared through the standardized CVE language. It enables connected ecosystem stakeholders to recognize their shared risks and collaborate to protect their shared resources. Most critically, it creates a positive feedback-loop among and between the Subcommittee's six interdependent priorities, and in doing so, increases desperately needed cybersecurity capabilities across society as a whole.

Committee Products: ISAC Roundtable and Public-Private Partnership Hearings (April 2017, June 2017)

Throughout the first half of 2017, the Subcommittee on Oversight and Investigations held several events focused on the public-private partnership model established under PPD-21. In the first, Committee Members and ISAC representatives discussed current ISAC challenges and opportunities. In the subsequent hearings, Members heard testimony from public and private sector representatives from the health care sector to examine how the sector can be made more effective and prepared for modern cyber threats.

VIII. Conclusion

This report represents the culmination of the Subcommittee on Oversight and Investigations' initial efforts to understand, explore, and ultimately address the cybersecurity challenges facing modern society. It recognizes that society today is so heavily dependent and so inextricably intertwined with the Internet and connected technologies that threats to the latter become immediate, serious threats to the former. Not only that, this report recognizes that there is no one "solution" to cybersecurity, but instead discrete yet interdependent policies that together create a holistic and effective strategy for dealing with the realities of modern cyber threats and opportunities.

Each of the concepts and priorities detailed here represent a piece of the broader cybersecurity challenge. Pursuing any one concept-priority pair in isolation will undoubtedly improve society's overall cybersecurity to some degree, but the Subcommittee's work over the past several years has shown that each concept-priority pair feeds off and builds upon its fellows. Further, as highlighted throughout this report, the Subcommittee has not simply identified important, high-level areas for future action, but has already begun to act. The work products associated with each concept and priority represent the Subcommittee's first steps towards implementing the policies it has identified.

More work remains to be done. The Subcommittee remains committed to strengthening the cybersecurity of the stakeholders under its jurisdiction, and will continue to pursue cybersecurity strategies and policies to enable the continued improvement of cybersecurity across society as a whole.