Dissertation

To Disclose, or Not to Disclose, That Is the Question

A Methods-Based Approach for Examining & Improving the US Government's Vulnerabilities Equities Process

Lindsey Polley

This document was submitted as a dissertation in February 2022 in partial fulfillment of the requirements of the doctoral degree in public policy analysis at the Pardee RAND Graduate School. The faculty committee that supervised and approved the dissertation consisted of John Bordeaux (Chair), Sasha Romanosky, and Quentin Hodgson.

PARDEE RAND GRADUATE SCHOOL

For more information on this publication, visit http://www.rand.org/t/RGSDA1954-1.

Published 2022 by the RAND Corporation, Santa Monica, Calif.

Abstract

This dissertation is the first publicly available methods-based approach to examining the previously classified Vulnerabilities Equities Process (VEP) – a federal level policy to adjudicate decisions on whether to retain or disclose newly discovered software vulnerabilities. Since its public acknowledgment in 2014, the benefits and shortcomings of the VEP have been sharply debated in the public arena by media, digital advocacy groups, and academia. The lack of publicly available data on the VEP, however, means that the majority of current public discourse is largely rooted in uninformed opinion. Two key aspects of this debate have focused on the design of the VEP charter itself, and the representation of equities considered during the vulnerability adjudication process. This dissertation analyzes the current VEP through a mixed methods approach and finds that – in both design and practice – it is deficient in its consideration of public-oriented equities and ethics that are important to software vulnerability-oriented public policy, directly impeding the current VEP's ability to promote social good through its adjudication process. I make eleven policy recommendations that address these deficiencies to support the VEP Director and Equities Review Board in making vulnerability adjudications that more robustly consider the equities of underrepresented stakeholders. This dissertation makes several original contributions to knowledge, including the development of a new virtue-based ethics framework for software vulnerability-oriented public policy. The development of this new framework not only fills a gap in the current literature, but also lays the foundation for further investigations into cyber policy and ethics – an under-researched yet critical nexus of modern life in a highly technology-dependent world.

Table of Contents

Figures

Tables

Executive Summary

This dissertation establishes recommendations for improving the Vulnerabilities Equities Process' (VEP) consideration of broad public interest and longer-term social good. The VEP is a federal-level policy designed to support the US Government in balancing the equities associated with the retention (and potential exploitation) and disclosure (and subsequent patching) of newly discovered software vulnerabilities. Although declassified in 2017, the VEP remains relatively unknown to the general public despite the fact that it has far-reaching ramifications for virtually every American citizen – and arguably, the international community as well. While the design of the VEP has been sharply debated by media, digital advocacy groups, and subject matter experts alike, there is very little publicly available data on the VEP. Most of the information that is available comes primarily from the VEP charter itself, along with a small number of public statements made by government officials; the majority of "information" currently available to the general public is largely rooted in opinion. Aside from limiting transparency, this absence of information inhibits policy researchers from drawing meaningful conclusions related to the current state or impact of the VEP. As a means of beginning to bridge this gap, this dissertation generates new information on the VEP by leveraging a mixed methods approach to examining the charter.

In Chapter 1, I trace the evolution of the VEP charter throughout the time it was classified, as well as the associated public discourse after the VEP's public reveal. In Chapter 2, I conduct interviews with VEP subject matter experts and key stakeholders centered around my findings from Chapter 1, and then perform an exploratory thematic analysis on the interview results. This thematic analysis highlights twelve emergent themes, including that the VEP – both in design and practice – is perceived to place greater emphasis on government-oriented equities than those of consumer and industry stakeholders. In Chapter 3, I design and apply a virtue-based ethics framework to the VEP, which yields similar results. Based on the findings and gaps highlighted across each method, I developed eleven policy recommendations (in bold below).

Infuse enforceability and accountability into the VEP through an Executive Order or National Security Memo. As it stands, the VEP charter is not technically enforceable; since there is no associated Executive Order or National Security Memo in place, compliance with the process cannot be compelled, and responsible parties cannot be held accountable for their actions. My research revealed that there is broad support across all stakeholder groups for the installation of a mechanism that would facilitate compliance with the VEP charter.

Begin producing the classified and unclassified annual reports as soon as possible, and clarify what should be included in said reports: Although the VEP charter commits to publishing both classified and unclassified versions of an annual report, my interviews confirmed that the unclassified reports are not being produced, while the classified reports are potentially

being delivered to members of Congress. Publishing said reports and better defining what they should include would increase transparency and public trust in the process.

Improve consumer and industry representation during ERB discussions by expanding Annex B and considering the implementation of an "additional representation mechanism": This study uncovered evidence supporting the claimed that the VEP charter – both in design and execution – currently does not adequately represent the equities of consumers and industry, even though government-oriented equities appear robustly represented. In order for the VEP to achieve its primary focus of "prioritiz[ing] the public's interest in cybersecurity,"[1] the representation of consumer and industry equities must be adequately considered during vulnerability adjudication discussions.

Expand "Part 4" of Annex B to address internationally oriented equities: While the VEP is a domestic-facing policy, the resulting vulnerability adjudications have potential implications for the broader international community – whose associated equities which are supposed to be represented on the ERB by the State Department, as well as through the VEP charter's Annex B. My interview results, however, support the claim that (1) a robust perspective on how vulnerability adjudications impact the US' international partnerships is currently not present in the ERB, and (2) there is no consideration given to how vulnerability adjudications may potentially impact civilian members of the international community.

Provide definitions or parameters within the charter that outline what constitutes a "demonstrable, overriding interest" for vulnerability retention: The current VEP charter states that it will only retain a vulnerability if there is "a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes,"[2] but does not provide parameters for what constitutes a "demonstrable, overriding interest." If a minimum standard or threshold for what constitutes an overriding interest is not established, then there is no way to enforce or ensure that the threshold of "overriding interest" is in fact being appropriately fulfilled and met with consistency.

Provide insight into how non-ERB members are notified to claim equity in a vulnerability under review: In addition to all ten permanent ERB members, any additional US Government entities that can demonstrate equity in a vulnerability submitted through the VEP for review is allowed to join the adjudication discussions. The current VEP charter, however, does not discuss how or through what channels non-ERB members are notified of a vulnerability under review – presenting a potentially significant gap in the representation of equities for entities that may not have received appropriate notification in the first place.

Provide more defined handling and follow-on processes to support expeditious vulnerability remediation: The "Handling & Follow-On Actions" section of the current VEP

[1] White House, 2017b, p. 1.

[2] White House, 2017b, p. 1.

charter is vague, lacking sufficient structure to be able to hold ERB members accountable. To improve accountability, (1) a more defined timeline for vulnerability disclosures following a dissemination decision should be established, (2) disclosure guidelines should be outlined within the charter to ensure consistency, and (3) and a more defined process, expectations, and timeline for the vendor follow-up should be installed.

Add a new "Annex D" that includes the virtue-based ethics framework developed in this dissertation to guide ERB ethics considerations: The results from applying my virtue-based ethics framework – which I developed – to the ERB suggests that the VEP is currently unable to adhere to ethics considerations that are important to software vulnerability-oriented public policy, which directly impedes its ability to promote longer-term social good through its vulnerability adjudications. Including my virtue-based ethics framework under a new "Annex D" would support ERB self-assessments, as well as provide the VEP Director with more contextualized findings regarding the ERB's adherence to ethics considerations and solutions to guide charter updates that promote social good.

An additional policy outside of the VEP should be put in place that focuses on the purchasing of vulnerabilities and exploits: The US Government is known to purchase software vulnerabilities from third-party vendors. These purchases are often accompanied by a Non-Disclosure Agreement, which public stakeholder groups (e.g., media, digital advocacy groups) believe prevents purchased vulnerabilities from being reviewed through the VEP; my interview results supported this concern, while also noting that are legitimate national security reasons linked to the continued purchasing and use of such vulnerabilities. Given the VEP's charter, however, the VEP and ERB meetings are not the appropriate venues for making decisions on this topic. As such, a stand-alone policy clarifying the US Government's stance on the appropriate parameters around the purchasing and use of third-party vulnerabilities should be released.

The VEP should remain focused on software vulnerabilities: My interview results highlighted that even though the cyber domain will continue to evolve and present the US Government with new challenges, it is important that the VEP remain focused on software vulnerabilities and not be required to expand their scope of review to other types of technology or technology application.

The US Government should actively engage other countries in designing & implementing their own VEP policies: As the cyber domain (as a domain of warfare) has continued to mature, my research highlighted that there are only four countries with publicly acknowledged VEP-like policies in place. Given the evolving threat landscape and global distribution of power, it is in the US Government's strategic interest to use its unique position and experience in the cyber domain to educate and work with our partners and other countries to develop their own VEP-like policies as a way to influence cyber norms in a direction that is beneficial to the US.

Acknowledgments

I've focused my doctoral research on the intersection of cyber policy and ethics in an effort to help develop a foundation for a safer and more equitable digital future in a world where the digital and physical realms are becoming increasingly intertwined. Although a difficult intersection to examine, I truly believe public policy efforts and further research in this area are crucial to ensuring a more stable, sustainable, and healthy future for the next generations. And President John F. Kennedy's quote captures my sentiment exactly: "We do these things not because they are easy, but because they are hard."

With that said, I could not have completed this difficult journey without the support of many colleagues, mentors, friends, and family. It is my privilege to thank as many as I can here, but I will not be able to thank them all. I hope everyone – both named and unnamed – know how very grateful I am for their support throughout these years.

First, I am incredibly thankful for the mentorship of my dissertation committee members: John Bordeaux, Sasha Romanosky, and Quentin Hodgson; each had high expectations of me and were generous with their time, despite being incredibly busy themselves. To John, thank you for supporting my passion for a topic that few others supported, for encouraging me to continue forward when times got tough, and for always providing hope throughout this lonely journey. To Sasha, thank you for challenging me throughout this process; our many conversations have made me a stronger and more thorough academic – qualities I will carry with me throughout the rest of my professional career. And to Quentin, thank you for your endless support since day one, for always providing constructive critiques that supported my intellectual growth, and for being an available source for all things cyber – despite the time of day or year.

I would also like to give a special thank you to Stephanie Pell – my outside reader. Despite your very busy schedule, you made time to not only read my dissertation, but to discuss the topic of cyber ethics with me on multiple occasions and at length. It was an honor to have you critique my research, and it is because of people like you that the field of cyber ethics will flourish.

There were several mentors I met along the way who helped make me the professional I am today. First and foremost, a special thank you to Ryan Consaul; you not only saw my potential, but also provided me with encouragement and numerous opportunities to grow as an academic – I promise to pay it forward. To Sarah Harting and Dan Gonzales, thank you for supporting and encouraging me to pursue topics I love; I genuinely hope our paths cross again. To Dave Baiocchi, Angel O'Mahony, Gery Ryan, and Rachel Swanger, thank you for helping me find my path when my doctoral journey experienced unexpected plot twists, and for encouraging my passion to make a difference; your unbridled support gave me the courage to pursue my dissertation topic – and for that support I am forever grateful. And to Ty Robichaux, thank you

for always believing in me and pushing me to not only dream big, but to achieve those dreams; a part of my success will always be because of your mentorship.

There were several PRGS doctoral fellows that supported me along my journey, but two in particular I would like to thank. First, to Claudia Rodriguez, thank you for not only being an amazing colleague, but an even more amazing friend; you supported me through both professional and personal struggles, spending many long hours tutoring me on every quantitative course we took – I would not have made it this far without your support and have genuinely enjoyed sharing this journey with you. And to Hilary Reininger, thank you for always "showing up" when I needed support; not only were you another cyber-focused fellow whom I could discuss methods and theory with, but you genuinely wanted to help me succeed, and for that I am blessed and grateful.

And of course, last but not least, the solid foundation that supported me throughout this entire journey: my family. To my mom, dad, grandparents, godparents, aunts, uncles, siblings, cousins, close family friends – of which there are *truly* too many to list – and my soon-to-be husband, I will never be able to thank you enough for the support and sacrifices that you too made in order to see me succeed – and for that I am sincerely and forever grateful.

Abbreviations

AI	artificial intelligence
CIA	Central Intelligence Agency
CNCI	Comprehensive National Cybersecurity Initiative
CVD	coordinated vulnerability disclosure
DC	Deputies Committee
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DoDIN	Department of Defense Information Network
EPIC	Electronic Privacy Information Center
ERB	Equities Review Board
EU	European Union
FBI	Federal Bureau of Investigations
FOIA	Freedom of Information Act
GOTS	government-off-the-shelf
HSC	Homeland Security Council
HSPC	Human Subjects Protection Committee
HSPD	Homeland Security Presidential Directive
IC	intelligence community
ISAC	Information Sharing and Analysis Center
LE	law enforcement
ML	machine learning
NDA	Non-Disclosure Agreement
NSA	National Security Agency
NSC	National Security Council

NSPD	National Security Presidential Directive
NSPM	National Security Presidential Memorandum
OMB	Office of Management and Budget
POC	point of contact
SME	subject matter expert
VDP	Vulnerability Disclosure Policy
VEP	Vulnerabilities Equities Process

Without a wholesome, systematic, and effective concept of social good, our public policy – no matter how vigorously implemented – will hardly succeed in accomplishing its task.

– Rajesh C. Shukla

Introduction

On the morning of June 6, 2013, the American public – along with the rest of the world – woke up to news that the US National Security Agency (NSA) had allegedly been indiscriminately collecting metadata from the telephone records of millions of Verizon customers, a large US telecommunications provider – an action allegedly being carried out legally under a classified court order.[3] This information was given to a journalist at *The Guardian* by a man named Edward Snowden who had previously worked as an intelligence contractor; this exchange marked the beginning of what would become known as the Snowden leak. Over the following years, roughly 7,000 pages[4] of alleged classified documents that Snowden is believed to have stolen from the NSA were published by journalists, outlining information regarding tools and methods, foreign officials and systems that had been targeted, encryption that had been broken, and the identities of companies and foreign governments that were allegedly cooperating with the NSA.[5] Altogether, the documents shed light into some of the NSA's largest signals intelligence programs that at times penetrate industry and the global community,[6] including the PRISM Program[7] (which allegedly provided the NSA, via the Federal Bureau of Investigation [FBI], with access to user data from nine large American technology and social media companies without users' knowledge), and Boundless Informant[8] (a data analysis and visualization tool which allegedly provided the NSA with situational awareness into the volume of signals intelligence being generated from each country). The Snowden leak had a profound and lasting impact on how the American public viewed government surveillance and privacy in the digital age. A large majority of the public began to distrust the government's access to and use of private citizens' data[9] – a distrust that also extended to the US judicial system and members of industry who the public viewed as complicit in the NSA's alleged intelligence gathering efforts.[10]

Almost one year later, on April 7, 2014, news of a serious software vulnerability in the popular OpenSSL cryptographic software library spread around the globe.[11] Dubbed

[3] Greenwald, 2013.

[4] Snowden is believed to have stolen roughly 1.5 million documents in total (Kelley, 2014.).

[5] Lawfare, n.d.

[6] Gallagher, 2018.

[7] Farivar, 2013.

[8] Greenwald & MacAskill, 2013.

[9] Hesseldahl, 2015.

[10] Geiger, 2018.

[11] Lee, 2015.

"Heartbleed," this vulnerability allowed attackers to eavesdrop on internet communications and steal data directly from compromised service providers and users.[12] With the Snowden leak and alleged NSA surveillance revelation still fresh in the public's memory, various media sources began reporting that the NSA had known about the Heartbleed vulnerability for several years and failed to disclose it for patching in order to exploit it for other intelligence gathering programs.[13, 14, 15, 16] In response, the NSA, White House, and the Director of National Intelligence (DNI) all denied these accusations, stating that no entity within the Federal Government had been aware of the Heartbleed vulnerability prior to its public disclosure.[17, 18, 19] In the eyes of the media, however, this denial of knowledge around such a catastrophic vulnerability – if true – highlighted potential widespread institutional weaknesses in how the Federal Government was approaching and implementing their policies to securing cyberspace – and this negative press continued to fuel the already-present public distrust.[20, 21]

Within days of Heartbleed's public disclosure, DNI's Public Affairs Office released an official statement that the "NSA was not aware of [Heartbleed]… until it was made public in a private sector cybersecurity report." Although this further fueled the media skepticism, it was two sentences at the end of this statement that would spark discussion on a new topic in the United States:

> "[The] White House has reviewed its policies in this area and reinvigorated an interagency process for deciding when to share vulnerabilities. This process is called the *Vulnerabilities Equities Process*."[22, 23]

What is the Vulnerabilities Equities Process (VEP), why haven't we heard about it before, and what impact does it have on the public? It was questions like these that spread through the media, digital advocacy groups, and research institutes alike in the weeks, months, and even years following the DNI's revelation of the VEP – a federal level process that, up until that point,

---

[12] Synopsis, 2020.

[13] Riley, 2014.

[14] Zetter, 2014.

[15] Sasso, 2014.

[16] Hosenball & Dunham, 2014.

[17] Wittes, 2014.

[18] Daniel, 2014.

[19] Office of the Director of National Intelligence, 2014.

[20] Whittaker, 2014.

[21] Sanchez, 2014.

[22] Office of the Director of National Intelligence, 2014.

[23] Italics added by author for emphasis.

had been classified and unknown to the public. It is against this backdrop of the Snowden leak, the Heartbleed discovery, and the revelation of the VEP that this dissertation begins.

Objectives & Policy Questions

This dissertation is the first publicly available methods-based approach to examining the Vulnerabilities Equities Process (VEP) – a federal-level policy designed to support the US Government in balancing the equities associated with the retention (and potential exploitation) and disclosure (and subsequent patching) of newly discovered software vulnerabilities. Although still relatively unknown to the general public, the VEP policy has far-reaching ramifications for all American citizens – and arguably for the international community as well. Through this study, I aim to better understand how the VEP considers broad public interest and longer-term social good throughout the adjudication process, and what – if any – gaps exist.

Important related policy questions include: How are "cyber vulnerabilities" defined within the VEP's framework, and are there emerging circumstances which would require us to adjust this definition? Which stakeholder interests are considered within this framework, and how are they represented or expressed? Who is responsible/informed/accountable/consulted in this decision-making process, and who has the ultimate decision authority? In practice, is the current VEP process bias or insufficiently robust given the criteria outlined in its charter? Is longer-term social good considered as a decision variable in the VEP's framework, and if not, should it be? Are any alternative frameworks currently employed by other countries, and if so, do they incorporate any variables that the US VEP does not account for?

Structure of This Dissertation

I begin this study by taking an in-depth look at the current VEP charter in Chapter 1. This includes tracing its evolution through the Federal Government during the time it was classified, as well as performing a comprehensive study of the public discourse around the VEP as it evolved. I then complete a review of proposed legislation related to the VEP to see how many bills were introduced to Congress for consideration, what their key objectives were, and how many (if any) made it to codification. To add perspective to my research on the US VEP, I then review how other countries (as of December 2021) are formally addressing the topic of equities-based vulnerability review at the national level.

In Chapter 2, I proceed with a qualitative approach to better understand the current state of the VEP by interviewing VEP subject matter experts (SMEs) on two key areas of interest identified in Chapter 1; this includes questions related to the mechanics of the VEP charter, as well as questions related to how equities are considered during the Equities Review Board (ERB) adjudication process. Once completed, I performed an exploratory thematic analysis on the interview results, which produced a robust set of findings centered around twelve emergent themes.

In Chapter 3, I assess the VEP using another method: the application of an ethics-based framework to the ERB (the VEP's decision-making entity). I begin by performing a brief review of how ethics have been applied to cyber-related public policy and discuss the importance of ethics in an increasingly digital society. Through this review and discussion, I identify the notable absence of an ethics-based framework specifically designed for application to software vulnerability-centric public policy. In order to continue with my assessment, I develop a virtue-based ethics framework and apply it to the ERB.

In Chapter 4, I outline eleven policy recommendations based on the findings and gaps highlighted across each method from the previous three chapters. These recommendations are divided into three over-arching categories: (1) recommendations for the VEP charter, (2) recommendations to improve the performance of the VEP, and (3) strategic recommendations related to the VEP.

Chapter 1: The Vulnerabilities Equities Process: Its Evolution, Public Critiques, & How Other Countries Are Approaching the Topic

The Evolution of the VEP

The first iteration of what would become the publicly released *Vulnerabilities Equities Policy and Process for the United States Government* was derived from the "National Security Presidential Directive (NSPD)-54 / Homeland Security Presidential Directive (HSPD)-23."

"National Security Presidential Directive 54" & "The Comprehensive National Cybersecurity Initiative"

On January 8, 2008, the George W. Bush Administration issued National Security Presidential Directive (NSPD)-54[24] in an effort to establish a comprehensive, national-level approach to securing cyberspace. A more holistic approach which better organized and aligned US Government response mechanisms was needed to combat the growing sophistication around cybersecurity threats. The goal was to not only protect National Security Systems, Federal systems, and private-sector critical infrastructure from *current* cyber threats, but to also anticipate *future* cyber threats and technologies that could compromise these networks. The need for this improved coordination – both for proactive and responsive efforts – resurfaced publicly in 2005 when a number of agencies across both the United States and United Kingdom Governments were compromised in a series of cyber operations largely attributed to Chinese Government-sponsored actors; this string of intrusions became collectively known as "Titan Rain" and was believed to have begun as early as 2003, although not publicly acknowledged until 2005.[25] In order to begin moving the relevant agencies and components in the necessary direction to effectively execute national-level cybersecurity coordination, an authoritative document providing a unified direction forward was needed. The signing of NSPD-54 provided this authoritative mandate, striving to provide a defined path forward[26] in three key ways:

1. By establishing the US Government's stance on the actions necessary to secure cyberspace by establishing associated policies, strategies, and guidelines.

[24] White House, 2008.

[25] Council on Foreign Relations, n.d.

[26] Since this study is focused on the VEP, research into the degree to which NSPD-54 accomplished its mandate has not been conducted.

2. By improving the coordination of the Federal Government's technical and organizational capabilities by (1) defining roles and responsibilities of the agencies involved, (2) outlining policy coordination and implementation actions, and (3) establishing a common (albeit minimal) lexicon of cybersecurity terms.
3. By establishing the view of cyber threats as having lifecycles – a series of strategic steps (or events) taken by a malicious actor that can be deterred, prevented, detected, characterized, attributed, monitored, and interdicted by the Federal Government.

Together, the "Comprehensive National Cybersecurity Initiative" (CNCI) carried out this whole-of-government approach. Detailed in NSPD-54, the Director of National Intelligence (DNI), Homeland Security, the Attorney General, and the Director of OMB (in coordination with the Secretaries of State, Treasury, Defense, Commerce, and Energy "as appropriate") monitored, coordinated, and recommended actions for the CNCI.[27] NSPD-54 states that in order for CNCI to be considered successful, these entities had ten main objectives they must achieve:

1. A report on CNCI implementation activities (including DNI recommendations) must be produced every three months and delivered to the President. The report must be delivered through the Assistant to the President for National Security Affairs, and the Assistant to the President for Homeland Security and Counterterrorism.
2. Ensure there are sufficient domestic resources in place to "neutralize, mitigate, and disrupt illegal computer activity".[28, 29]
3. Increase the US Government's understanding of current and future foreign cyber advancements (including technological advancements) through the use of predictive, behavioral, information, and trend analyses.[30]
4. Increase our cybersecurity and information assurance efforts to (1) protect National Security Systems from unauthorized access, and (2) facilitate greater cross-government information sharing.[31]
5. Determine which data and applications on unclassified Federal networks are most at risk to being altered, stolen, or destroyed – and recommend their migration to a more secure network.[32]

---

[27] White House, 2008.

[28] White House, 2008, p.13.

[29] The responsibility of the Secretary of Homeland Security and the Attorney General.

[30] The responsibility of the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the DNI, and other Federal agencies when deemed necessary by the before mentioned entities.

[31] The responsibility of the Secretary of Defense and the DNI.

[32] The responsibility of the Director of OMB, with assistance from the heads of all executive agencies and departments. Must be completed within 180 days of the directive's release.

6. In the defense of US networks, develop a joint plan for the use and synchronization of offensive measures.[33] This plan must be submitted to the Assistant to the President for National Security Affairs, and the Assistant to the President for Homeland Security and Counterterrorism.
7. Develop a plan to better coordinate and implement the law enforcement capabilities available to support the investigation of cyber incidents occurring on US networks.[34]

The remaining three objectives – and many other parts of NSPD-54 – are still classified.

On March 4, 2008 – roughly a month after NSPD-54 was issued – several government officials testified before the Senate Homeland Security and Governmental Affairs Committee in a closed hearing on the role of the Department of Homeland Security (DHS) in the CNCI, linked to a cybersecurity budget increase request from DHS.[35] While the committee overall supported DHS' increased role in protecting Federal computer networks, the near-triple budget increase request did receive scrutiny. As part of this scrutiny, Senators Joe Lieberman and Susan Collins sent a public letter to Michael Chertoff (the Secretary of DHS at the time) on May 1, 2008, which requested answers to several follow-up questions, citing that an "increased openness and information sharing with Congress, the private sector, and the American public [would] aid in the eventual success of the initiative." [36] Although this open letter was one of the first glimpses the public received into the CNCI and NSPD-54, it did not receive much press until 2009 with the transition into the Obama Administration.

As one of his first actions in office, President Obama directed a Cyberspace Policy Review of the Federal Government's plans, programs, and activities within cyberspace (meaning the communications and information infrastructure); the National Security Council (NSC) and the Homeland Security Council (HSC) carried out this review and assessed how well these efforts were being integrated, resourced, and coordinated.[37] As part of the final Cyberspace Policy Review report, the review team found that the CNCI originally put in place by the George W. Bush Administration had been an appropriate first step and should become a key element from which a broader, updated national cyber policy should evolve. [38] President Obama ultimately accepted this recommendation and released the full Cyberspace Policy Review in May 2009. In-

[33] The responsibility of the Secretaries of State, Defense, and Homeland Security, the DNI, and the Attorney General. Must be completed within 120 days of the directive's release.

[34] The responsibility of the Attorney General and the Secretary of Homeland Security, in coordination with the Secretary of Defense and the DNI. Must be completed within 120 days of the directive's release.

[35] U.S. Senate Committee on Homeland Security & Governmental Affairs, 2008.

[36] U.S. Senate Committee on Homeland Security & Governmental Affairs, 2008.

[37] The NSC and HSC had 60 days from the date of the directive to complete this review and provide the President with a final report.

[38] White House, 2009.

depth information specifically related to the CNCI, however, would not be available until March 2010, when the Obama administration released a summary explanation of the CNCI to boost transparency and public understanding of the Federal effort.[39]

The combination of these events – beginning with the open letter submitted by Senators Joe Lieberman and Susan Collins, and culminating with President Obama's release of the Cyberspace Policy Review which acknowledged the CNIC– ultimately triggered a Freedom of Information Act (FOIA) request by the Electronic Privacy Information Center (EPIC) – a self-described non-profit research and advocacy center focused on emerging privacy and civil liberties issues in the digital age.[40] EPIC formally submitted their FOIA request to the National Security Agency (NSA) on June 25, 2009[41] seeking the text, executing protocols, and related privacy policies of NSPD-54. This request, however, would not be granted until June 5, 2014 – nearly five years later, following lengthy legal proceedings between EPIC and the NSA.

Within that timeframe, however, a new document emerged: the *Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process*, issued February 16, 2010.[42]

"Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process"

Issued on February 16, 2010 – and classified at the time – the "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process" marked the first official iteration of the VEP. It was conceptualized and developed during a working group led by the Obama administration's Director of National Intelligence following the Cyber Policy Review of 2009.[43] The structure and contents of this original VEP appear to have been very similar to that of the current VEP, although less detailed. It is difficult, however, to tell exactly how different the two iterations are from one another, primarily because approximately fifty percent of the "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process" remains redacted.

This original VEP would remain unknown to the general public until 2014 when the Office of the Director of National Intelligence's Public Affairs Office released an official statement in response to the public backlash resulting from the emergence and public dissemination of the

---

[39] White House, 2010.

[40] Electronic Privacy Information Center, n.d.a.

[41] Electronic Privacy Information Center, n.d.b.

[42] White House, 2017b.

[43] Ambastha, 2019.

Heartbleed[44] vulnerability. In the statement delivered by the Public Affairs Office, it was divulged that "an interagency process for deciding when to share vulnerabilities [exists, and] is called the Vulnerabilities Equities Process."[45] This revelation sparked an immediate reaction from media and digital advocacy groups alike, and ultimately resulted in at least two FOIA requests – one by the EPIC (mentioned in the previous section) and another by the Electronic Frontier Foundation (EFF) – a self-described non-profit research center focused on civil liberty issues in the digital age.[46, 47] After a series of separate and lengthy back-and-forth legal proceeding between EPIC and the NSA / ODNI, and EFF and the NSA / ODNI, a heavily redacted version of the "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process" was released in January 2016. Attention on this document would be short-lived, however, as the updated VEP charter would be released a year later.

Emergence of the Current VEP Charter

Between the time the "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process" (the original iteration of the VEP) had been established and the public reporting of the Heartbleed vulnerability, the original VEP had fallen dormant.[48] Heartbleed (and to some degree, the remaining fallout from Snowden), however, reinvigorated this effort, ultimately resulting in the updating of the VEP's charter and its public release in 2017 under the Trump Administration.[49]

This updated VEP charter addressed many of the criticisms[50] voiced about the original charter and was largely applauded by the media for its increased transparency regarding how the US Government approaches a subset of cyber domain events. Despite these improves, though, certain criticisms remained.

Criticisms of the "Early" VEP

The early VEP – including the documents and initiatives that led up to the VEP, such as NSPD-54 – were generally viewed as first steps in the right direction by members of the Federal

---

[44] Please refer to the "Introduction" section of this report for more information on the Heartbleed vulnerability.

[45] Office of the Director of National Intelligence, 2014.

[46] Electronic Frontier Foundation, n.d.

[47] Electronic Frontier Foundation v. National Security Agency, Office of the Director of National Intelligence, 2016.

[48] Quote from interviewee: "The VEP had been on a long list of things that we wanted to restart, but it was until about 2013, 2014 after Snowden and Heartbleed that we were actually able to stand it back up and rewrite the charter."

[49] Office of the Director of National Intelligence, 2014.

[50] Refer to the "Criticisms Of The Original VEP" and "Criticisms Of The Current VEP" sections of Chapter 1 for an in-depth discussion on this topic.

Government who were aware of them (given that they were all classified at the time of their establishment); they marked the designation of cybersecurity as a national priority, and established policies, strategies, and guidelines for a critical area that lacked Federal-level coordination. With that said, though, once the documents were declassified and entered into the public's view, criticisms began to surface.

Perhaps the most widely expressed criticism was the perceived "lack of transparency"[51, 52, 53, 54, 55] on behalf of the government towards the public regarding the contents of these formative documents – meaning that the public (as voiced through media outlets and digital advocacy groups) believed that the Federal Government was not sharing information around the existence of these policies and process with them when they should be; some of this may be attributable to bad timing, as a wave of public distrust regarding the Federal Government's digital activities (particularly as they relate to the US population) was still present from the Snowden leak in 2013.[56] One key driver behind this lack of transparency, though, was the fact that these documents were all classified at the time of their development, and unclassified versions – or even unclassified summaries – were generally not available, making it difficult for anyone who was not directly involved to understand what the true policy stances were, what the processes looked like, or what the policies did – or did not – cover. Again, this limited public knowledge and uncertainty around whether such policies even existed (let alone what they contained) was compounded by the underlying concern that without adequate transparency (e.g., knowledge of the guidelines, decision-makers, etc.), the public could not hold the Federal Government accountable for their actions and decisions around the retention or disclosure of vulnerabilities.[57, 58, 59, 60]

Many reporters and members of digital advocacy groups criticized the "early" VEP for not codified into law, often viewing it as a loophole to avoiding the process altogether. Without a legal requirement for the existence of (or compliance with) the VEP through an Executive Order or statute, many within the media and digital advocacy groups questioned how – or if – compliance was enforced, and whether or not the equities involved were being adequately

---

[51] Peterson, 2013.

[52] AccessNow, 2016.

[53] Schneier, 2016.

[54] Gillmor & Honeywell, 2017.

[55] Electronic Frontier Foundation v. National Security Agency, Office of the Director of National Intelligence, 2016.

[56] Klein et al., 2016.

[57] Pell & Finocchiaro, 2017.

[58] Center for Internet and Society, 2016.

[59] Wilson et al., 2016.

[60] Klein et al., 2016.

balanced with each decision. Without an enforcing mechanism, there were fears that the decisions around the retention or disclosure of vulnerabilities would be left to "the officials in the negotiating rooms"[61] to determine if the charter would be implemented at all – leading many within the media and digital advocacy groups to worry that it would ultimately fade away completely.[62, 63, 64, 65, 66] These two stakeholder groups also viewed Non-Disclosure Agreements (NDA) in particular as a means of avoiding the VEP process altogether after then-FBI Director Comey referred to the VEP during a press conference as "an informal process set up inside the government" which excluded NDAs-related vulnerabilities from review.[67, 68]

The fact that the guidelines used to make vulnerability retention or disclosure decisions were still not publicly available was another criticism that echoed in the media – bringing the issue of accountability back up. Many within the media and digital advocacy groups felt that if the public did not have access to the guidelines themselves, they could not hold the government accountable and ensure they were not being put in an unnecessary amount of risk. Similar sentiments were brought up by members of Congress who were concerned that the Administration's unwillingness to declassify details of the VEP (and CNCI) did not allow for adequate congressional oversight.[69] These same members of Congress emphasized the necessity for the US Government to collaborate with other critical components, the private sector, and outside experts in order to successfully protect American citizens and Federal Government networks.[70]

Since the vulnerability retention or disclosure guidelines were not available, critics turned to the tone of the VEP as a potential proxy. Some within the media and digital advocacy groups believed that the classified guidelines would reflect the VEP's lack of a clear "pro-disclosure" policy, and that worried people – especially in the context of vulnerability stockpiling.[71] Industry stakeholders, cybersecurity professionals, and the media broadly viewed vulnerability stockpiling as a bad government practice, and were worried that the VEP's guidelines did not

---

[61] Newman, 2017b.

[62] Pell & Finocchiaro, 2017.

[63] Center for Internet and Society, 2016.

[64] Wilson et al., 2016.

[65] Senate Committee on Armed Services, 2016.

[66] Schwartz & Knake, 2016.

[67] Comey was asked by a reporter why the FBI had not submitted an Apple vulnerability ultimately that was used to access one of the San Bernardino shooter's iPhones to the VEP.

[68] Federal Bureau of Investigation, 2016.

[69] U.S. Senate Committee on Homeland Security & Governmental Affairs, 2008.

[70] U.S. Senate Committee on Homeland Security & Governmental Affairs, 2008.

[71] Gates, 2017.

address the issue.[72] These stakeholders feared that the longer vulnerabilities sat on a shelf instead of being disclosed to the public or vendors for patching, the more likely it became that the public could be exploited by adversaries who may have also discovered the same vulnerabilities.[73, 74, 75]

There were a select few from within the intelligence community, however, that did not agree with this stance and believed that the VEP should actually default to a policy of vulnerability retention over fears that disclosure may signal US capabilities to adversaries.[76] I could not locate any public commentary from this particular stakeholder group regarding their stance on vulnerability stockpiling.

A final common critique focused on who the decisionmakers were in the VEP, and how many of those decisionmakers were from the intelligence community. Some within the media and digital advocacy groups were skeptical that decisionmakers from the intelligence community with dual roles of both supporting cybersecurity as well as exploiting vulnerabilities discovered to further their intelligence mission would have competing interests or agendas when it came to a disclosure or retention decisions, which could potentially skew decisions in a way that was not in the best interest of the public.[77] Some within the media believed that the role of the Executive Secretariat should not be filled by the NSA simply given the amount of negative media they had sustained over alleged mishandlings of cyber vulnerabilities in the past.[78] For a small number of critics from within the intelligence community, however, the VEP injected an unnecessary amount of uncertainty into the workflow of intelligence officers managing vulnerability exploitation and intelligence gathering activities for the Federal Government.[79] The claim here is that by removing the intelligence professionals from the decision-making loop and replacing them with an "inexpert intergovernmental oversight" body (referring to the ERB), intelligence officers lose the ability to make potentially time sensitive tactical decisions and instead have to wait until the ERB reviews their vulnerability to see if they will be able to exploit the new access point (the vulnerability), which ultimately impacts their workflow.[80]

From these critiques emerged a consistent set of recommendations for how the Federal Government could not only improve the process, but do so in such a way that increased public trust and confidence in the process:

---

[72] Smith, 2017a.

[73] Center for Internet and Society, 2016.

[74] Gates, 2017.

[75] Braga, 2017.

[76] Aitel & Tait, 2016.

[77] Braga, 2017.

[78] Schwartz & Knake, 2016.

[79] Aitel & Tait, 2016.

[80] Aitel & Tait, 2016.

1. **Enshrine the VEP into law**: In order to strengthen transparency, oversight, and accountability of the process, the VEP should be written into law either via an Executive Order or by Congress, and should require the review of VEP membership, process, criteria, and guidelines. It should also require government-wide compliance.[81, 82, 83, 84]
2. **Clearly outline and publicly release the VEP process and guidelines:** This should include making the high-level process and decision-making criteria for vulnerability disclosure or retention public, and should default towards disclosure (with retention being a rare exception).[85, 86]
3. **Clearly outline and publicly disclose which agencies are involved in the VEP**: This includes entities involved in the process, but should also specifically call out which entities have a vote in the "disclosure versus retention" decision. [87]
4. **Transfer the Executive Secretary function from NSA to another agency**: In an effort to distance the VEP from the negative media around the NSA and any potential conflict of interest, the Executive Secretariat role should be transferred to another agency – such as the Department of Homeland Security.[88]
5. **Require a periodic review of any vulnerabilities retained through the VEP**: The VEP should establish clear guidelines on the re-assessment of retained vulnerabilities to evaluate their suitability for disclosure to mitigate the number of vulnerabilities being unnecessarily stockpiled for long periods of time.[89, 90]
6. **Prohibit agencies from entering into NDAs**: NDAs allow agencies that purchase vulnerabilities to circumvent the VEP. Prohibiting NDAs would eliminate a large loophole that potentially places the public and vendors in an unnecessary amount of risk.[91, 92]
7. **Require annual reporting**: This report should provide a status update on the VEP program to Congress and the public, and should consist of both a high-level publicly available section and a classified annex for relevant congressional committees.[93, 94]

---

[81] Senate Committee on Armed Services, 2016.

[82] Schwartz & Knake, 2016.

[83] Klein et al., 2016.

[84] Wilson et al., 2016.

[85] Schwartz & Knake, 2016.

[86] Baras et al., 2011.

[87] Klein et al., 2016.

[88] Schwartz & Knake, 2016.

[89] Schwartz & Knake, 2016.

[90] Klein et al., 2016.

[91] Wilson et al., 2016.

[92] Schwartz & Knake, 2016.

[93] Klein et al., 2016.

[94] Schwartz & Knake, 2016.

It was not long after these criticisms around the original VEP charter began to emerge, however, that the current VEP charter was released in 2017. The following sections outline the structure of the current VEP charter along with associated the public discourse at the time.

The Structure of the Current VEP

Purpose & Objective

Through the course of carrying out missions, research, or other work, different components of the US Government uncover previously unknown software vulnerabilities (also known as "zero-days") that could potentially be exploited by threat actors for nefarious reasons; alternatively, these vulnerabilities could also be leveraged by the US Government for intelligence gathering or operational purposes that support US national security interests. But as our world has become more interconnected and dependent on the cyber domain, coordination of the exploitation or patching of these zero-days through a standardized and pre-designated process became necessary. The establishment of the VEP supports coordinate cyber activities through the informed evaluation of competing considerations and equities associated with the dissemination or retention of newly discovered software vulnerabilities.[95]

As stated in the updated charter, the VEP's primary objective during these risk versus benefit discussions is to "prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy."[96] In theory, the VEP should demonstrate this prioritization by tending towards the disclosure of vulnerabilities to vendors for security patching (as mentioned in the charter), unless there is a "demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes."[97]

Participants & Stakeholders

Entities participating within the VEP fall into one of four categories: a permanent member of the Equities Review Board (ERB), a temporary participant with the ERB, the VEP Director, or the VEP Executive Secretariat.

Per the VEP charter, the following entities are considered permanent members of the ERB:

- Office of Management and Budget (OMB)
- Office of the Director of National Intelligence (to include Intelligence Community-Security Coordination Center (IC-SCC))
- Department of the Treasury

[95] White House, 2017.

[96] White House, 2017.

[97] White House, 2017.

- Department of State
- Department of Justice (to include the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force (NCIJTF))
- Department of Homeland Security (to include the National Cybersecurity Communications and Integration Center (NCCIC) and the United States Secret Service (USSS))
- Department of Energy
- Department of Defense (DoD) (including the National Security Agency (NSA) (including Information Assurance and Signals Intelligence elements)), United States Cyber Command, and DoD Cyber Crime Center (DC3))
- Department of Commerce
- Central Intelligence Agency (CIA)

Any other US Government agency that can demonstrate responsibility for – or equity in – a vulnerability under review by the ERB is permitted to become a temporary participant with the ERB – although the VEP charter does not indicate how non-permanent ERB members (e.g., an agency that is not already an ERB member) are notified in order to have the chance to demonstrate equity in a given vulnerability and participate in the discussion process. If granted permission to participate, such an agency would also be required to select one individual authorized to represent the views of the respective agency head at the relevant ERB meeting.

Each of the abovementioned entities – including any temporary ERB members – must select one individual authorized to represent the views of their respective agency head at each monthly ERB meeting, where members of the ERB deliberate – and make determinations – on vulnerabilities that have met the threshold for review (this threshold criteria will be reviewed in the following "Review Process" section). Furthermore, each agency is required to select one individual to act as their agency's point of contact (POC). This POC has three main responsibilities:

1. Receive vulnerability submissions from their respective agency for submission to the ERB.
2. Identify a minimum of one subject matter expert (SME) from their respective agency to support equities determinations and related ERB discussions as needed.
3. Serve as the VEP Director's primary contact for their respective agency.

The position of VEP Director is held by the same individual serving as the Special Assistant to the President and Cybersecurity Coordinator[98] – or an equivalent successor if necessary. The main responsibility of the VEP Director is to ensure that all VEP policies are being efficiently and effectively implemented.

[98] As of 2021, this position may now be held by the recently established National Cyber Director.

The final role of VEP Executive Secretariat defaults to the NSA. This role, however, can be delegated to another agency by the VEP Director, as long as the head of said agency agrees to take on this role. Regardless of which agency fills the function of the VEP Executive Secretariat, they will – at all times – remain under the authority, direction, and control of the Secretary of Defense. The main objectives of the VEP Executive Secretariat are:

- To facilitate the flow of information, discussions, determinations, and documentation throughout the VEP;
- To maintain formal records of these events, information, and determinations so that efficacy reviews of the overall process can be performed at a later date; and
- To perform these functions in a way that is neutral and independent.

On top of achieving these main objectives, the VEP Executive Secretariat is responsible for carrying out four key duties:

1. Collect and retain the contact information for each agency's VEP POC, SME, and ERB members.
2. Maintain records of all vulnerabilities that have been submitted to (or identified by) the VEP Executive Secretariat; these records should capture (at a minimum) the agency who submitted the vulnerability, the dissemination determination and its accompanying date, and whether reassessment of the vulnerability is necessary.
3. Development and submission of the VEPs annual report.
4. Document the contested preliminary determination process of the VEP, and retain for future reference.

The Review Process

The VEP is triggered once a vulnerability identified by a US Government agency meets the threshold for equities review by the ERB. In order to meet this threshold, a vulnerability[99] must be both:

1. ***newly discovered***: defined by the VEP as a zero-day vulnerability or new zero-day vulnerability information not previously known by the US Government prior to its submission;[100] and
2. ***not publicly known***: meaning that the vendor has not yet been made aware of the vulnerability, and/or that information about the vulnerability cannot yet be found in the public domain.[101]

---

[99] The VEP defines a *vulnerability* as "A weakness in an information system or its components (e.g., system security procedures, hardware design, internal controls) that could be exploited or impact confidentiality, integrity, or availability of information." (White House, 2017, p. 12.)

[100] White House, 2017, p. 11.

[101] White House, 2017, p. 12.

Once an agency determines that a given vulnerability *does* meet this review threshold, the vulnerability is submitted to the VEP Executive Secretariat. This submission includes information describing the vulnerability, identifies any products or systems that are vulnerable as a result of the vulnerability, and provides a preliminary recommendation on how information on this vulnerability should be further disseminated.

After receipt of a vulnerability submission, the VEP Executive Secretariat has one business day to notify all VEP POCs from permanent ERB member agencies of the vulnerability; again, the VEP charter does not indicate how non-permanent ERB members who may have an equity claim are notified so they can request participation in relevant meetings. Each respective agency then has five business days to come forward and claim equity in the submitted vulnerability. Any agencies that do claim equity must also formally state whether they concur with the preliminary recommendation on dissemination made by the original submitting agency. If – during this step in the process – one or more agencies claiming equity do *not* agree with the preliminary recommendation made by the original submitting agency, a meeting will be held between (1) the SMEs from the submitting agency, (2) the representative and SMEs from the non-concurring agencies, and (3) the VEP Executive Secretariat. These entities then have seven business days to discuss and come to a consensus on how the vulnerability should be handled. If a consensus cannot be reached, each party must submit options to the ERB for further review and discussion.

The VEP process is designed to help VEP participants and the ERB reach a consensus on the final determination of vulnerabilities under review. If – after the previous steps – the ERB itself cannot reach a consensus, a preliminary determination is made by the ERB via a vote. At this point, if none of the VEP participants contest the preliminary determination, it is adopted as the "final determination" and any follow-on actions begin. However, if an agency who previously demonstrated equity in the vulnerability under review does *not* agree with the preliminary determination made by the ERB, they have the opportunity to formally challenge (or "contest," which is the formal term used in the charter) the decision before any actions are carried out.

In some instances, a preliminary determination made by the ERB may result in a policy concern on the part of the Executive Office of the President – although the parameters around what may qualify as a "policy concern" is not outlined or discussed in the charter. In this event, the VEP Director will take those concerns back to the ERB for further discussion.

Challenges & Disputes within the VEP

An agency wishing to contest a preliminary determination made by the ERB has five business days to formally notify the VEP Executive Secretariat of their intent to contest, and include the reasons for their challenge. The VEP Executive Secretariat, in turn, must notify the VEP Director that a challenge to the preliminary determination has been made.

When a VEP participant – including any agency who has demonstrated equity in a vulnerability under review – formally submits these statements, the challenge is resolved through the processes put in place by the National Security Presidential Memorandum (NSPM)-4 of April

4, 2017. Under NSPM-4,[102, 103] these discussions take place at either a NSC[104] meeting, a HSC[105] meeting, a Principals Committee[106] meeting, or a Deputies Committee[107] (DC) meeting – whichever is most appropriate as determined by the President's National Security Advisor and the NSC staff; the Chief of Staff to the President (or a delegate) is part of the NSC staff and is

[102] This section condenses the actual system put in place by NSPM-4 for national security policy development and decision making. For an in-depth understanding of the process, please refer to the National Security Presidential Memorandum–4 document in the References (National Security Presidential Memorandum–4, 2017).

[103] It is worth noting that each administration may issue their own Presidential Memorandum outlining national security decision-making processes; for example, NSPM-4 was released by the Trump Administration, while National Security Memo 2 (NSM-2) was released by the Biden Administration. While the names of these documents may change and a handful of involved agencies may be updated, these overall processes generally remain the same.

[104] The NSC – per the National Security Act of 1947, as amended – is responsible for advising the President of the United States on items related to the integration of domestic, foreign, and military policies relating to national security. (White House, 2017a.)

[105] The HSC – which was established through Executive Order 13228 of October 8, 2001, and codified in the Homeland Security Act of 2002 – is responsible for advising the President of the United States on items related to homeland security. (White House, 2017a.)

[106] The Principals Committee is a Cabinet-level senior interagency forum where policy issues affecting the national security interests of the United States are discussed. The Principals Committee is convened and chaired by the National Security Advisor (unless these responsibilities are delegated by the National Security Advisor to the Homeland Security Advisor). The National Security Advisor is also responsible for preparing the agenda for each meeting, in consultation with other committee members as appropriate. Members of the Principals Committee include: the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Energy, the Secretary of Homeland Security, the Chief of Staff to the President, the Director of National Intelligence, the Chairman of the Joint Chiefs of Staff, the Director of the Central Intelligence Agency, the National Security Advisor, the Homeland Security Advisor, the Representative of the United States to the United Nations, the Counsel to the President, the Deputy Counsel to the President for National Security Affairs, the Director of the Office of Management and Budget, the Assistant to the President, the Deputy National Security Advisor, the Deputy National Security Advisor for Strategy, the Deputy Assistant to the President, the National Security Advisor to the Vice President, and the Executive Secretary (otherwise known as the "Chief of Staff"). When appropriate given the agenda, the Assistant to the President for Intragovernmental and Technology Initiatives, the Secretary of Commerce, the United States Trade Representative, and the Assistant to the President for Economic Policy may also attend. (White House, 2017a.)

[107] The Deputies Committee is a senior sub-Cabinet interagency forum where policy issues that impact the national security interests of the United States are discussed and – where appropriate – are decided on. The Deputies Committee is convened and chaired by the Deputy National Security Advisor (unless these responsibilities are delegated by the Deputy National Security Advisor to the Deputy Homeland Security Advisor). The agenda for these meetings is prepared by the Deputy National Security Advisor in consultation with other committee members as appropriate. Members of the Deputies Committee include: the Deputy Secretary of State, the Deputy Secretary of the Treasury, the Deputy Secretary of Defense, the Deputy Attorney General, the Deputy Secretary of Energy, the Deputy Secretary of Homeland Security, the Deputy Director of the Office of Management and Budget, the Deputy Director of National Intelligence, the Vice Chairman of the Joint Chiefs of Staff, the Deputy Director of the Central Intelligence Agency, the Deputy National Security Advisor, the Deputy National Security Advisor for Strategy, the Deputy Homeland Security Advisor, the Deputy Assistant to the President and National Security Advisor to the Vice President, the Administrator of the United States Agency for International Development, the Chief of Staff, and the Deputy Counsel to the President for National Security Affairs. Other senior officials may be invited by the Deputy National Security Advisor as appropriate. (White House, 2017a.)

present to accurately represent the views of the President.[108, 109] The DC is responsible for reviewing and monitoring any work done through these interagency national security channels, and ensures that any issues – including those arising from the VEP or ERB – are properly analyzed and prepared for decision-making. Once a decision has been made, the Chief of Staff to the President is responsible for ensuring that any necessary papers are prepared, and that the final decisions are promptly communicated to the VEP Director and VEP Executive Secretariat.

Any other disputes that arise during the VEP follow the same process outlined above.

Equity Considerations

In order to construct a comprehensive understanding of the potential risks a vulnerability under review may pose to current and near-future US national security and national interests, four core categories of equities are considered before a determination is made: (1) Defensive equities, (2) Intelligence, Law Enforcement, and Operational equities, (3) Commercial equities, and (4) International Partnership equities. The VEP charter's outlining of these categories suggests that these four stakeholder groups compose the core of what the US Government believes to be representative of the "public interest" or "public good."

Defensive Equities

As the VEP charter is written, defensive equities appear to receive the most comprehensive review when compared to the other three categories. Under this part of the equities review, the potential risk posed by a vulnerability is assessed across four separate dimensions: threat, vulnerability, impact, and mitigation.

The "threat" dimension is meant to help VEP participants gain an understanding for how likely the threat created by the vulnerability under review is to materialize. This includes understanding the range of products or equipment compromised by the vulnerability (specifying the versions, if necessary), and how widely used they are (including what systems and industries they are linked to). This dimension also tries to determine how likely a threat actor is to exploit the vulnerability if they are in fact aware of it. [110]

The "vulnerability" dimension is meant to help VEP participants gain an understanding for how likely it is that a threat actor would *actually* be able to exploit the vulnerability under

---

[108] White House, 2017a.

[109] The NSC staff serves both the NSC and the HSC. It consists of regional, issue-focused, and functional directorates, and is headed by the Chief of Staff (in accordance with 50 U.S.C. 3021). (White House, 2017a.)

[110] The mere existence of a vulnerability does not guarantee that it will be exploited by a threat actor. There are many reasons why a threat actor might choose not to exploit a certain vulnerability, such as (1) the investment required to reach a point of access where the vulnerability can be exploited (e.g., reconnaissance, use of other zero-days, etc.) may be too high, (2) the potential payoff may not be worth the exploitation of a new zero-day (noting that once a zero-day is exploited, the likelihood of knowledge of its existence goes up, increasing the likelihood that it will be patch and therefore unusable in the future), and (3) there may be other known vulnerabilities that the target is not protected against that are easier to exploit. (Heckman, 2016)

review. This includes information around the level of access a threat actor would need within a system in order to exploit the vulnerability, what other vulnerabilities or information a threat actor would need in order to cause harm,[111] and how likely it is that a threat actor would in fact be able to acquire the abovementioned knowledge in order to exploit the vulnerability under review.

The "impact" dimension is meant to help VEP participants gain an understanding for the level of disruption that could potentially result from the vulnerability being exploited. This includes identifying how reliant users are on the compromised product or system, how severe the vulnerability is, what type of consequences could result if the vulnerability was exploited (e.g., the failure of a key system upon which critical infrastructure is reliant to distribute resources or perform services), and the benefit a threat actor could gain from exploiting the vulnerability. Under this section, reviewers also consider that if a patch for the vulnerability *is* developed and disseminated publicly, is it likely that enough US Government entities, commercial entities, and consumers will actually install the patch in order to offset the harm posed to security; and what the likelihood is that a threat actor would be able to reverse engineer the patch in order to uncover the vulnerability and then use it against unpatched systems.

The "mitigation" dimension is meant to help VEP participants understand what actions or mechanisms are currently in place (or could be put in place) to eliminate or reduce the risks and potential impacts posed by the vulnerability under review. These include (but are not limited to) mechanisms, best practices, security practices, configurations, software patches, or system updates. If a software patch or system update is being considered, reviewers must determine:

1. If the vulnerability is disclosed, how likely is it that a vendor, research institution, or other entity will develop a patch or update? And how long would it take?
2. How likely is it that the patch or update will be effective (including how effective)?
3. What percentage of vulnerable systems will have the patch or update applied within a year once it is made available? What percentage will apply the patch or update sooner, and what percentage will never have the patch or update applied?

This dimension also addresses the question of whether or not US Government entities – or other members of the defense community – would be able to detect if the vulnerability under review was exploited by a threat actor – either in retrospect or in potential future exploitation events.

Intelligence, Law Enforcement, and Operational Equities

The equity considerations around intelligence, law enforcement, and operations are designed to support VEP participants in understanding the impacts that a vulnerability under review could potentially have on related entities and activities. Under this part of the equities review, the

[111] In some cases, no other vulnerabilities or information are needed in order for a threat actor to cause harm by exploiting the vulnerability under review.

potential risk is assessed across two separate dimensions: operational value, and operational impact.

The "operational value" dimension is meant to help VEP participants gain an understanding for the ways in which the vulnerability under review may actually be leveraged as an asset – potentially in support of intelligence collection, cyber operations, or law enforcement evidence collection; this includes considering both the potential current and future value of exploiting the vulnerability. If it is determined that there is operational value gained from leveraging the vulnerability, the review team must consider if there are any ways to demonstrate this value, and the level of operational effectiveness that can be achieved via the use of the vulnerability.

The "operational impact" dimension is meant to help VEP participants gain an understanding of the *overall* impact that the exploitation of the vulnerability would have on operations. This includes (but is not limited to) considering:

1. Would exploitation of this vulnerability negatively impact threat actors and/or their operations?
2. Would exploitation of this vulnerability negatively impact any of the US Government's National Intelligence Priorities Framework priorities or military targets?
3. Are there any scenarios where exploiting the vulnerability would result in additional protection for US warfighters or civilians?

Additionally, this dimension must also consider whether there are any other means – outside of exploiting the vulnerability – that would result in the same operational benefits, and if disclosure of the vulnerability would reveal any intelligence sources or intelligence gather methods used by the US Government.

Commercial Equities

This part of the equities review is designed to help VEP participants understand the potential impacts that the exploitation of the vulnerability under review could have on the commercial sector. The review committee must also take into consideration how disclosure of this vulnerability – and, thus, acknowledgement of the US Government's knowledge of it – might affect the relationship between the US Government and industry. This section for consideration of commercial sector equities is noticeably smaller when compared to the depth of consideration given to the Defensive and Intelligence/Law Enforcement equities above.

International Partnership Equities

The final equities review focuses on the US Government's relationship with international partners and allies. Similar to the review focused on the commercial sector, this part of the review must address how the relationship between the US Government and its international partners would be impacted if it was revealed that the US Government had knowledge of the vulnerability.

Vulnerability Determinations: Disclose or Restrict?

Per the VEP charter, the determination process used to decide whether to disclose or restrict a vulnerability should be completed quickly (although "quickly" is not defined), in full consultation with all VEP participants (including those agencies who have demonstrated equity in the vulnerability), and in a way that considers the overall best interests of the US Government's mission and interests around cybersecurity, intelligence, counterintelligence, law enforcement, military operations, and critical infrastructure protection (as outlined in the *Equity Considerations* section above).

In addition to these discussions and equities reviews, determinations around disclosure or restriction should also be based on "repeatable techniques and methodologies that enable benefits and risks to be objectively evaluated by VEP participants."[112] These tests should be conducted in a way that supports the VEP participants' objective assessment of the potential risks and benefits of both disclosure and restriction of the vulnerability. For comprehensiveness, these tests should assess factors such as prevalence of the vulnerability, the US Government's reliance on the compromised systems (as well as its reliance on the vulnerability's potential offensive uses), and the severity of damage that could be caused by deciding to disclose or restrict knowledge of the vulnerability.

The final determination made on a vulnerability by the ERB will fall into one of two categories: *disclose* or *restrict*. Accompanying each final determination will be a set of agreed-upon guidelines that outline how the vulnerability will be handled, as well as any necessary follow-on actions.

A "disclose" determination means that the ERB has determined that disclosure of the vulnerability is in the overall best interest of the US Government's cybersecurity, intelligence, counterintelligence, law enforcement, military operations, and critical infrastructure protection missions. When a "disclose" determination is made, information about the vulnerability is disseminated to the vendor as soon as possible[113] by the entity that originally submitted the vulnerability to the VEP for review (now referred to as the "releasing entity"); the VEP charter assumes that the entity who first discovered the vulnerability is the most knowledgeable about it.[114] The releasing entity can also decide to delegate these dissemination responsibilities to another entity. Regardless of which entity disseminates the information, the dissemination guidelines that accompanied the final determination must be followed. Once the information has been disseminated, the releasing entity must submit a copy of all the information shared to the VEP Executive Secretariat for record keeping. Afterwards, the releasing entity must also follow-up with the ERB to determine if the vendor has taken appropriate and timely actions to patch (or

---

[112] White House, 2017b, p. 7.

[113] Dissemination of the vulnerability's information (per the final determination guidelines) must occur no later than seven business days after the final "disclose" determination is made. (White House, 2017.)

[114] White House, 2017b.

otherwise mitigate) the vulnerability in a way that meets the requirements laid out in the agreed-upon guidelines document. If the vendor chooses not to patch the vulnerability – or does so in a way that does not meet the requirements – the releasing entity must notify the VEP Executive Secretariat immediately, clearing the way for the US Government to pursue "other mitigation steps."[115] The charter does not provide examples or include a discussion as to what types of activities might constitute these "other mitigation steps."

Each vulnerability that receives a "restrict" determination will be reassessed annually for disclosure eligibility until:

1. The vulnerability receives a "dissemination" vote from the ERB and is disclosed to the appropriate vendor for patch development;
2. The vulnerability becomes publicly known through other means (e.g., discovered by a research institute, etc.); or,
3. The vulnerability is mitigated by other means.

Regardless of the final determination, the submitting agency is also responsible for engaging with other VEP participants to address various mitigation options, which – at times – may include engaging stakeholders outside of the US Government.

If a US Government entity discovers malicious activity that exploits a vulnerability that is under a "restrict" determination, the discovering entity must immediately notify the VEP Executive Secretariat. No later than one business day after the notification, the ERB must meet to reach a consensus on whether to (1) disclose the vulnerability so it can be mitigated by the vendor, or (2) take alternative mitigating actions.

It is worth noting that the decision to disclose or restrict vulnerability information – regardless of the situation – can be impacted by any restrictions in place between the US Government and other foreign or private sector partners. This would extend to any joint efforts or operations the US Government is engaged in with allies or coalition partners; if these partners have a vulnerability that they are actively exploiting (or planning to exploit), it is possible that the US Government may need to abide by any disclosure or retention restrictions put in place by these counterparts – even if it goes against an ERB adjudication decision.

Other types of restrictions that may impact a disclosure or retention decisions include Non-Disclosure Agreements (most commonly associated with vulnerabilities or exploits that a US Government entity purchases from a third party), Memoranda of Understanding, or other potential agreements limiting the US Government's actions when determining to disclose or restrict information about a vulnerability.

[115] White House, 2017b, p. 8.

Exceptions and Other Considerations

There are a select number of tightly defined categories of vulnerabilities that are exempt from the VEP process. The largest category are those vulnerabilities that are linked to restrictions due to partner agreements and sensitive operations. The exact details of these categories are outlined in the VEP charter's classified "Annex C." The number of vulnerabilities that receive a VEP process exemption must be aggregated and reported to the ERB at each meeting.

Other vulnerabilities exempt from a VEP review include:

1. **Vulnerabilities identified through security research or private sector incident response**: Per international standards and best practices, these vulnerabilities should be disclosed as soon as possible.
2. **Vulnerabilities resulting from misconfiguration**: This includes misconfiguration or poor configuration done in order to facilitate ease of use (e.g., disabling certain security features to "improve" functionality or limit performance issues); this is not necessarily considered a security flaw, but rather an operator error.
3. **Vulnerabilities resulting from unintended device use**: This includes the use of engineering, configuration tools, techniques, or scripts that increase or decrease a device's functionality for other than what the device was intended for.
4. **Vulnerabilities resulting from an unsecured device**: Devices or systems that lack any security protocols or feature will not be reviewed via the VEP; these are not "vulnerabilities" in the sense of what the VEP was designed to review, but rather are design flaws.

It should also be noted that the VEP explicitly mentions that it "is not intended to prevent the US Government from taking immediate actions to protect its network(s) or warn entities actively threatened by a malicious cyber event, including ongoing unauthorized access to information systems."[116] This suggests that the VEP charter has a level of flexibility built into its design to allow for both the restriction of a vulnerability coupled with other US Government actions in order to protect their networks.

Vulnerabilities Discovered in NSA-Certified Systems

If a vulnerability is located in a piece of government-off-the-shelf (GOTS) equipment or system that has been certified by the NSA, the NSA is responsible for reporting the vulnerability to the VEP Executive Secretariat. Similarly, if a vulnerability is located in a piece of hardware or software that performs a cryptographic function for the US Government, the NSA is responsible for formally submitting it to the VEP Executive Secretariat. This reference to GOTS equipment and NSA-certified systems appears to be specifically called out to clearly designate which entity

[116] White House, 2017, p. 3.

is responsible for reporting vulnerabilities to the ERB, given that GOTS and NSA-certified systems are used by multiple US Government entities.

Vulnerabilities Discovered by Non-US Government Entities

In some cases, vulnerabilities may be brought forward to a US Government entity by a private business, a research entity, or a foreign government. In these instances, the VEP charter directs the involved US Government entity to encourage the discoverer to either disclose the vulnerability (given international standards and best practices), and/or take additional mitigating actions to reduce the risk posed by the vulnerability.

Criticisms of the "Current" VEP

The current VEP charter was positively received by the public (as voiced by the media and digital advocacy groups alike), but still received criticism.[117, 118, 119] It appeared that many of the previous version's criticisms were heard and attempted to be addressed in this new iteration. The media in general applauded this updated charter for the sharp increase in transparency. This included a fully documented vulnerability review process, detailed lists of the agencies involved, detailed lists of the equity considerations used to make vulnerability disclosure/retention decisions, and a commitment to publish annual reports with metrics (both a classified and unclassified version).[120, 121, 122, 123, 124] With this increased transparency of the entire process, many within the media and digital advocacy groups believed that major players in the VEP could now be held more accountable for their actions, and the interests of all stakeholders would now be more fairly represented.[125, 126] The publication of annual reports would also enable a more open and productive discussion about how to assess and improve upon the VEP going forward.[127]

This new iteration of the VEP charter also received positive media for explicitly acknowledging that the exploitation of vulnerabilities poses a potential threat to civilians, their

---

[117] Crocker, 2017.

[118] Heller, 2017.

[119] Stisa Granick, 2017.

[120] Vijayan, 2017.

[121] Newman, 2017b.

[122] Knake, 2017.

[123] Tech Accord, 2018.

[124] Ambastha, 2019.

[125] Haracic, 2017.

[126] Crocker, 2017.

[127] Charlet et al., 2017.

individual privacy, and the economy – not simply through the blanket term of "national security."[128] Along these lines, the current VEP also indirectly addressed previous concerns around stockpiling vulnerabilities by committing to re-evaluate every vulnerability that is retained until it is finally disclosed.[129]

Despite these positive steps forward, however, the current VEP did encounter some negative criticism – the most prominent being that it had still not been codified into law, resurfacing questions around enforceability and compliance.[130, 131, 132] Concerns of potential loopholes around the VEP also remained. Not only was the use of NDAs not addressed by the current charter, but the current VEP also deemed vulnerabilities associated with "partner agreements" and "sensitive operations" as exempt from review; critics remarked that virtually any work tangentially related to law enforcement or defense might be intentionally mislabeled as a "sensitive operation" in order to avoid VEP review.[133, 134, 135, 136, 137]

The current VEP also received criticism from media and digital advocacy representatives for having the NSA continue as the VEP Executive Secretariat. There had been previous calls for this role to be delegated to a more neutral party, several indicating that a good alternative would be the Department of Homeland Security (DHS)[138,139, 140] – although it is worth noting that is it unclear if DHS would in fact be a neutral party given that they also have potentially conflicting cybersecurity, intelligence, and law enforcement components. Although this lack of re-assignment was viewed as a "bad public relations move,"[141] the VEP did include a new clause that allows the White House Cybersecurity Coordinator to "designate another agency to perform this function with the permission of the head of that agency," [142] as long as the function can still

[128] Vijayan, 2017.

[129] Newman, 2017b.

[130] Newman, 2017b.

[131] Knake, 2017.

[132] Zhang, 2019.

[133] Vijayan, 2017.

[134] Knake, 2017.

[135] Crocker, 2017.

[136] Ambastha, 2019.

[137] Zhang, 2019.

[138] Healey, 2016.

[139] Schwartz & Knake, 2016.

[140] Knake, 2017.

[141] Knake, 2017.

[142] White House, 2017, p. 4.

be executed in a neutral and independent way.[143] Similar criticisms emerged regarding the VEP's commitment to annual reporting; although generally viewed as a step forward by media and digital rights advocates, there was desire for a commitment to include more granular information and meaningful descriptions, including the severity of the vulnerabilities retained, and the amount and severity of vulnerabilities purchased.[144, 145]

A fair amount of the current VEP charter's criticism focused on the topic of "equities." The current VEP did improve from the initial version by including an extensive list of VEP members and equity considerations used to make vulnerability disclosure/retention decisions. Although many critics within the media and digital advocacy groups were relieved to see entities like the State Department, Treasury, Department of Commerce, and Department of Energy had been added to the VEP members list to represent other priorities and viewpoints, the concern lingered that the majority of member entities came from the intelligence community – including the Department of Defense, the Department of Homeland Security, and the Department of Justice.[146] In addition, several critics noted the lack of involvement of elected representatives, members of the private sector, or an entity that focuses on civilian consumer security and protection – all of which would be appropriately postured to represent the interests of citizens.[147, 148] The equities considerations listed in the current VEP were also criticized as "requiring too many assumptions that leave room for potential bias to enter the decision making process."[149] Many within the media and digital advocacy groups wondered how the VEP calculates or otherwise assesses the economic and security impact of the vulnerabilities discovered or purchased, and whether it also addresses the long-lasting impacts and cleanup efforts required when a vulnerability is left in the public (i.e., "retained") and exploited by an adversary.[150]

A final concern – which is related to the previous point on equities considerations – focused on whether the VEP violated the privacy rights of users. Predominantly voiced by digital and civil rights activists, there were concerns that because the actual process lacked, oversight, legal accountability, and privacy guidelines (referring to guidelines that would protect the digital privacy of users from unlawful intrusion) for the federal entities involved, they could be gaining access to customers' personal data (which would otherwise require a warrant to access).[151]

---

[143] Newman, 2017b.

[144] Ambastha, 2019.

[145] Zhang, 2019.

[146] Newman, 2017b.

[147] Ambastha, 2019.

[148] Zhang, 2019.

[149] Zhang, 2019.

[150] Tech Accord, 2018.

[151] Because this concern is linked to the operational use (or exploitation) of a software vulnerability after it has gone through the VEP, it falls outside of the scope of this research.

It is worth noting here that I was unable to locate any of the unclassified annual reports that the VEP charter commits to producing, nor was I able to locate any reference to the classified versions that are supposed to be sent to Congress annually as well. Perhaps equally as interesting is that the criticisms I discussed above do not acknowledge the absence of these annual reports.

Industry and the VEP

Industry has never been identified as a formal participant in any iteration of the VEP (although their engagement by participating agencies is not explicitly prohibited). Many industry stakeholders, however, have expressed the opinion that their lack of involvement in the VEP unnecessarily exposes both the public and service providers to systemic, long-term risk. Two of the most vocal members of industry on this topic have been Mozilla and Microsoft.

Mozilla

Founded in 2003, the Mozilla Foundation (and its subsidiaries) is a non-profit public benefit software development organization dedicated to developing open-source and free end user products – including browsers to support a more accessible internet – that evolved out of the Mozilla software community established in 1998 by members of Netscape[152] and is guided by a set of principles (called "The Mozilla Manifesto") in their effort to make the internet "a better place for everyone."[153]

Mozilla initially began publicly commenting on the VEP in 2016 following several cyber related events stemming from vulnerabilities, including cyber attacks on the Democratic National Convention and state electoral systems. Mozilla declared that the Federal Government has the responsibility to disclose vulnerabilities to the affected vendors as they become aware of them so that patches can quickly be developed. While acknowledging that there are legitimate reasons for delaying disclosure, Mozilla claimed that not doing so puts billions of users at risk (including Mozilla's government users), as well as the vendor's infrastructure. And that as the amount of time between discovery and disclosure increased, so too did the amount of risk incurred by users and vendors, given that the likelihood that others (including adversaries) had also discovered the vulnerability (and, therefore, may have already exploited it) increased as well. Mozilla believed that these two interests – retention by the government versus disclosure for patching – must be balanced, and that truly solving this problem would require industry and government to work together. This, however, would require the government to put transparency and accountability

[152] Mozilla, 2005.

[153] Mozilla, n.d.

policies in place, such as codifying the VEP, implementing a standard set of criteria for decision making, and independent oversight.[154, 155]

The 2017 WannaCry ransomware attack pushed Mozilla to become more vocal about their stance, arguing that the attack highlighted why government-industry partnerships regarding vulnerability disclosures and security updates are so important. They highlighted that although Microsoft had discovered related vulnerabilities back in March of 2017 and had provided patches, not all users had applied the patches – which was a key reason why the WannaCry attack was so prolific. Mozilla criticized the government, stating that if the vulnerabilities linked to WannaCry had been disclosed to Microsoft sooner, the patches could have been released earlier and in a coordinated manner to encourage users to apply the patches. If the government insists on retaining vulnerabilities, they must begin accounting for the associated long-lasting and rippling effects of not disclosing a given vulnerability in time.[156]

The WannaCry attack also gave Mozilla another reason to re-engage in their VEP advocacy, arguing that if the VEP had been codified, then the related vulnerabilities may have been disclosed in time to help mitigate some of the fallout. In addition to reiterating the need for the VEP's codification, Mozilla highlighted that the process' current domination by intelligent community and law enforcement entities required an increase in transparency and oversight (lead by an independent entity), and the inclusion of a civilian consumer security and protection agency to ensure that advocates of civilian equities are not excluded.[157] They also asserted that the VEP process should be housed within DHS, positing that they are more appropriately postured to facilitate interagency deliberations, information sharing, and disclosure processes than the NSA and the Special Assistant to the President and Cybersecurity Coordinator.

Mozilla became a staunch supporter of the *Protecting Our Ability to Counter Hacking (PATCH) Act* which was introduced into the House of Representatives in May of 2017. The PATCH Act addressed many of the transparency, reporting, consideration gaps, and codification concerns that Mozilla had been writing about for the past year.[158, 159] When the current VEP was released in November of 2017, Mozilla mostly praised the changes as a step in the right direction, especially around the increase in transparency around the process as a whole. They were, however, disappointed that their concerns around the VEP's codification were still not addressed.[160]

---

[154] Dixon, 2016.

[155] West, 2016.

[156] Dixon, 2017b.

[157] Mozilla, 2017.

[158] West, 2017a.

[159] Dixon, 2017a.

[160] West, 2017b.

Microsoft

Founded in 1975, Microsoft is a technology company widely known for computer software, consumer electronics, and personal computers. As they have grown and permeated the technology landscape, Microsoft stood up a government partnership office in order to support efforts that make cyberspace safer for the public.[161] In the early 2000s, Microsoft began several internal initiatives in an effort to better-protect their users. Two of these initiatives included the Microsoft Threat Intelligence Center and the Digital Crimes Unit which help identify and assess vulnerabilities, including criminal activities leveraging vulnerabilities in their products and services, and have adopted proactive testing and analytics practices to enable rapid IT infrastructure updates.

In February of 2017, amid growing frustration with how governments were approaching the retention of cyber vulnerabilities, Microsoft's President Brad Smith argued that an international Digital Geneva Convention was needed to commit governments to protect civilians from nation-state cyber attacks in times of peace (echoing the sentiment of how the Fourth Geneva Convention protects civilians in times of war). As part of his argument, Smith offered the following six points as core tenets of the proposed Digital Geneva Convention[162]:

1. No targeting of tech companies, private sector, or critical infrastructure.
2. Assist private sector efforts to detect, contain, respond to, and recover from events.
3. Report vulnerabilities to vendors rather than to stockpile, sell, or exploit them.
4. Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable.
5. Commit to nonproliferation activities to cyberweapons.
6. Limit offensive operations to avoid a mass event.

Smith argued that similar to how the Fourth Geneva Convention recognized the participation of the Red Cross as an integral part of civilian protection during times of war, the technology industry was now being put in a similar position – increasingly becoming the internet's "first responders." Because of this growing responsibility, tech companies should assume a neutral position and agree to take collective action to make the internet a safer place for all users.[163]

In the wake of WannaCry, Smith once again echoed his belief of tech companies' increasing role as first responders to cyber attacks, and – as a result – stated that Microsoft and other companies in similar positions have a responsibility to respond. Smith went one step further and called upon users to do their part to help mitigate the fallout of such attacks by applying security updates as soon as they are released by a vendor. In Smith's opinion, the WannaCry attack had highlighted the degree to which cybersecurity was no longer simply a vendor's responsibility, but

[161] Microsoft, n.d.

[162] Smith 2017a.

[163] Smith 2017a.

the responsibility of both the vendor *and* customers; the fact that many computers remained vulnerable to the WannaCry vulnerabilities even two months after patches had been released illustrated this fact.[164] When assessing the US Government's level of responsibility in the WannaCry outbreak, Smith discussed that this was not an isolated event, but rather a pattern of activities with ill-assessed and unintended consequences that culminated in the 2017 outbreak. Smith lays out his opinion in the following quote:

> "This attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem... We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen."[165]

Microsoft has been working to develop closer and more formalized relationships with government and law enforcement entities to be able to more rapidly share the intelligence gathered on vulnerabilities and cyber criminals through these internal efforts; similar efforts to boost transparency around discovered software vulnerabilities and criminal activity with the public have been ongoing.[166] A recent example of how all these internal efforts work together occurred in January 2020, when the NSA and Microsoft jointly revealed a critical vulnerability in the Microsoft Windows operating system and urged organizations and the public to quickly apply a security update (prepared in advance of the public release) that effectively patched the vulnerability.[167, 168] A similar example occurred as recently as March 2021, in which the NSA again informed Microsoft of a set of critical vulnerabilities that could have been exploited to remotely compromise their Exchange Server email software program. [169] This prompted the swift release of a security update by Microsoft, along with a message to the public regarding the nature of the vulnerability and the alleged Chinese state-sponsored actor responsible for exploiting the vulnerability.[170]

---

[164] Smith, 2017b.

[165] Smith, 2017b.

[166] Smith, 2017b.

[167] Martinez, 2020.

[168] Collier, 2020.

[169] Lyngaas, 2021.

[170] Burt, 2021.

The Federal Government & Industry: Learning How to Play Together

Even though industry has not been given many formal tools by the Federal Government to support in the securing of cyberspace and the protection of users, we have seen coordination between the two increase (as some of the examples above highlighted). This coordination, however, has continuously been overshadowed by the question of "when is it appropriate to disclose a vulnerability?" – and the answer to that question largely depends on which side of the spectrum your entity exists on.

A good example that illustrates how much of a "grey area" vulnerability disclosure can be began in 2013 when media outlets reported that the United States' Federal Bureau of Investigations (FBI) was leveraging a vulnerability in Mozilla's Firefox 17 browser to identify and charge providers, promoters, and distributors of "illegal goods" – unbeknownst to Mozilla.[171, 172] Almost immediately, Mozilla released a public response stating that they had been made aware of a potential security vulnerability in their Firefox 17 browser and were investigating to learn more – an indication that the FBI had not coordinated with Mozilla in advance.[173] As Mozilla pressed the FBI for information regarding the vulnerability so it could be patched, they were met with resistance from the government because the FBI was using this vulnerability to target individuals sexually exploiting children on the dark web – and they wanted to be able to continue to use it. Many within the public (as reported on by the media) viewed the FBI's explanation for not disclosing the vulnerability to Mozilla as a reasonable justification; and while Mozilla never argued against that point, they did fear that since the vulnerability had now gained global publicity, it needed to be patched or would inevitably also be exploited by cybercriminals against innocent users of their browser.[174] Despite several pleas to the FBI directly and several federal court orders (which were ultimately overturned), the FBI has not disclosed the vulnerability to Mozilla (or any of the other similar vulnerabilities since 2013, such as the leaked Exodus exploit in 2016[175]), leaving many within the cybersecurity community to wonder whether the vulnerability is still being exploited.[176, 177, 178] While the FBI ultimately arrested approximately 900 individuals and rescued approximately 350 abused children worldwide as a result of these Mozilla vulnerabilities (dubbed "Operation Pacifier"), it went to great lengths in order to prevent the vulnerabilities' disclosure – even dropping at least one

---

[171] Cox, 2016b.

[172] Krebs, 2013.

[173] Mozilla, 2013.

[174] Kirk, 2016.

[175] Brewster, 2016.

[176] Cox, 2016a.

[177] Lee, 2016.

[178] Booth, 2016.

indictment in order to keep it a secret – and received public criticism for allowing the site to continue to operate as they identified perpetrators.[179, 180, 181, 182]

What was so important about this FBI-Mozilla example is that it provided the joint government-industry stakeholder community with one of the most difficult use cases possible – both in terms of the sheer moral dilemma it presented, but also with respect to user privacy.[183] It prompted digital and civil rights activists alike to question (1) whether a third party (such as Mozilla, in this case) should be allowed to intervene and disclose a vulnerability in order to protect users, and (2) whether evidence gathered through the use of such vulnerabilities should be admissible in court (effectively circumventing the need for warrants).[184, 185]

A recent example, however, that highlights a high degree of coordination, more clear-cut lines, and industry's desire to rise to the occasion occurred in October 2020 with the coordinated takedown of TrickBot botnet[186], a command and control network of compromised computers used to spread malware. First reported in 2016, TrickBot started as a piece of malware focused on online banking credentials theft, but quickly evolved in scope and ability, ultimately infecting more than one million devices and becoming the world's largest global network.[187, 188] At the time, there was growing fear that – in addition to the large amount of funds being stolen from institutions and individuals alike – the giant botnet would be used to compromise the 2020 Presidential Elections by locking up state and local computer systems or altering election counts.[189] In a tightly coordinated effort between Microsoft and other members of the Financial Services Information Sharing and Analysis Center, Microsoft obtained a court order from a federal judge in the Eastern District of Virginia which gave Microsoft legal control of TrickBot, allowing Microsoft to disable the IP addresses used by TrickBot's command and control servers,

---

[179] Newman, 2017a.

[180] Federal Bureau of Investigation, 2017.

[181] Christian, 2019.

[182] Rumold, 2016.

[183] Edwards, 2019.

[184] Rumold, 2016.

[185] Electronic Privacy Information Center, n.d.c.

[186] A "botnet" (short for "robot network") is a network of compromised or hijacked computers and devices that is infected with malware that allows for the attacker or hijacker to remotely controlled the entire network of compromised devices to launch attacks designed to crash a target's network, inject malware, harvest credentials, and/or execute CPU-intensive tasks. (CrowdStrike, 2020) (TrendMicro, n.d.)

[187] Microsoft, 2020.

[188] Cybersecurity & Infrastructure Security Agency, 2021a.

[189] Greene & Nakashima, 2020.

effectively rendering those servers and their content inaccessible to the botnet's operators.[190, 191, 192] While there were still lessons to be learned from this effort and areas where additional coordination could have occurred (as it turned out, the United States Cyber Command had begun a separate but parallel effort in September 2020 to hack into TrickBot's command and control servers – unbeknownst to Microsoft), this example is largely viewed as a success story for how industry can not only step up and make a positive contribution to the security of the cyber realm, but can do so in a coordinated manner with legal authorities.

Proposed & Related Legislation

Since the public revelation of the VEP's existence by the Director of National Intelligence in 2014, only a handful of legislative efforts related to the VEP have been introduced to Congress.

Protecting Our Ability to Counter Hacking (PATCH) Act

Introduced into the House of Representatives in May 2017 under the 115th Congress – and then referred to the House Committee on Oversight and Government Reform – the PATCH Act[193, 194] would have codified the existence of a "Vulnerability Equities Review Board." This federal-level entity would be formally responsible for providing the public with "the policies related to whether, when, how, to whom, and to what degree information about a vulnerability in a technology, product, system, service, or application that is not publicly known should be shared or released by the government to a non-federal entity;" these policies would also be submitted to the President and Congress, and would include a description of any anticipated challenges that would require legislative or administrative action to overcome.

Furthermore, the PATCH Act would require all federal agencies to submit any information regarding a vulnerability to the Vulnerability Equities Review Board, who would then determine if the vulnerability should undergo their formal dissemination/public release determination process. If the Vulnerability Equities Review Board determines that a vulnerability does not need to go through a formal review, the involved federal agencies would be permitted to publicly release the vulnerability information.

The formal vulnerability review process completed by the Vulnerability Equities Review Board would include the following considerations, at a minimum:

---

[190] Sanger & Perlroth, 2020.

[191] Constantin, 2020.

[192] Fung, 2020.

[193] 115th Congress, 2017b.

[194] I reached out to U.S. Representative Ted Lieu (D-Calif.) on August 31, 2021, who was one of the bipartisan sponsors of this Act, but as of the time of publication of this study I did not receive a response.

- "Which technologies, products, systems, services, or applications are subject to the vulnerability;
- the potential risks of leaving the vulnerability unpatched or unmitigated;
- the likelihood that a non-federal entity will discover the vulnerability; and,
- whether the vulnerability can be patched or otherwise mitigated."

If it is determined that information about a vulnerability should be disclosed to the respective vendor for patching, then the Vulnerability Equities Review Board would be obligated to notify DHS.

The proposed PATCH Act ultimately died under the 115th Congress after being introduced into the House of Representatives. Although the PATCH Act did not make it past the House Committee on Oversight and Government Reform, its introduction into the House of Representatives was significant because it marked the first time that Congress became "actively involved in meaningful discussion about government disclosure of vulnerabilities." [195]

Cyber Vulnerability Disclosure Reporting Act

Originally introduced in July 2017, the Cyber Vulnerability Disclosure Reporting Act[196] aimed to aggregate the policies and procedures developed for coordinating disclosures about cyber vulnerabilities within DHS, and then provide the results to the Committee on Homeland Security and Governmental Affairs in a public report. Under the proposed act, the Secretary of Homeland Security would have 240 days to compile the policies and procedures used to disclose cyber vulnerabilities in the previous year into the main body of a report (which must be unclassified), and include an annex (that can be either unclassified or classified) that outlines information on the degree to which information about the disclosed vulnerabilities were acted upon by industry and/or other stakeholders. In addition, this report *may* also include a description of how the Secretary is coordinating efforts with other Federal entities and critical infrastructure owners and operators to prevent, detect, and mitigate cyber vulnerabilities.

After being re-introduced into the House of Representatives in January 2021, the proposed Cyber Vulnerability Disclosure Reporting Act ultimately died under the 117th Congress.

[195] Fidler & Herr, 2017.

[196] 115th Congress, 2017a.

50 U.S. Code § 3316a – Reports on intelligence community participation in vulnerabilities equities process of Federal Government

50 U.S. Code § 3316a[197] outlines parameters for reports on intelligence community participation in federal-level vulnerabilities equities processes in three key sections – Section A, Section B, and Section C. Section A establishes definitions for:

- **Vulnerabilities Equities Policy and Process documents:** refers to the executive branch document entitled "Vulnerabilities Equities Policy and Process," dated November 15, 2017.
- **Vulnerabilities Equities Process:** refers to the interagency review of vulnerabilities, pursuant to the Vulnerabilities Equities Policy and Process document or any successor document.
- **Vulnerability:** defined as a weakness in an information system or its components (e.g., system security procedures, hardware design, and internal controls) that could be exploited or could affect confidentiality, integrity, or availability of information.

Section B outlines key parameters for reports related to the VEP process and criteria. Under this section, the Director of National Intelligence has a maximum of 90 days (from December 20, 2019) to provide the congressional intelligence committee with a report that:

1. Lists the title of the official(s) responsible for determining whether a vulnerability is submitted to the VEP – for each member of the intelligence community;
2. The process that each designated official uses to make their determination; and,
3. The roles and responsibilities of each intelligence community member during a VEP vulnerability review.

Section B also states that a description of any significant changes made to the processes or criteria used to make a vulnerability review determination must be submitted to the congressional intelligence committees within 30 days of the change, and that all reports must be unclassified (but may include a classified annex).

Section C outlines annual reporting parameters, requiring that a minimum of one classified report be submitted to the congressional intelligence committees by the Director of National Intelligence regarding developments from the previous year, and should call out:

1. The number of vulnerabilities submitted for review under the VEP;
2. The number of vulnerabilities disclosed to vendors for patching (must also be included in an unclassified annex);
3. The number of vulnerabilities disclosed to the public (must also be included in an unclassified annex); and,

[197] 50 U.S. Code § 3316a, 2019.

4. The total number of vulnerabilities – by category – that were determined to be exempt from review by the VEP.

Finally, the Director of National Intelligence does not have to submit an annual report if another annual report which contains all the necessary information has already been submitted to Congress.

It is worth noting that this particular development appears to have gone unnoticed by the public, as I was unable to locate reference to it in any public VEP-related conversations.

How Are Other Countries Handling Vulnerability Disclosure?

At the time of this dissertation's composition (December 2021), very few countries had a publicly available national-level vulnerabilities equities process in place to determine whether a newly discovered vulnerability should be disclosed to vendors for patching or retained by the government for future use. Recently, however, an increasing number of entities are calling for international creation and harmonization of national-level vulnerability disclosure policies (sometimes referred to as "government disclosure decision process" [GPPD]) – even citing international standards ISO/IEC 30111:2013 on vulnerability handling processes and 29147:2014 on vulnerability disclosure as beneficial starting points.[198, 199] Members of the European Union (EU) have particularly been vocal about the topic and have advocated for the EU to "outline specific principles for member states to follow in developing a European vulnerability equities process with clear priority given to reporting vulnerabilities to vendors," suggesting that this role could be effectively performed by ENISA, the European Union's Agency for Network and Information Security.[200, 201] The possibility of an EU-focused VEP has been discussed recently at various forums, including the Global Forum on Cyber Expertise[202] and the Carnegie Endowment for International Peace.[203] In the interim, though, the Centre for European Policy Studies (a think tank focused on EU affairs) has been vocal in encouraging member states to adopt their own equity-based vulnerability review processes.[204] While there are still only a small number of countries with VEP-like policies in place, a larger number of countries are beginning to design and implement Coordinated Vulnerability Disclosure programs

[198] Pupillo, 2017.

[199] Herpig & Schwartz, 2019.

[200] Pupillo, 2017.

[201] Charlet et al., 2017.

[202] Global Forum on Cyber Expertise, n.d.

[203] Carnegie Endowment for International Peace, 2018.

[204] Pupillo, 2017.

which facilitate the communication of vulnerabilities from the private sector to government. The following sections dive deeper into the current state of both of these categories.

Countries With VEP Policies

At the time of this dissertation's composition (December 2021), Australia, Canada, and the United Kingdom were the only countries outside of the United States that had publicly acknowledged and available VEP policies. Note that all four countries are of the Anglosphere and have long-spanning intelligence sharing relationships, perhaps making it more explainable as to why the VEP policies of all four countries are strikingly similar and place their intelligence agencies as leads for their VEP processes.[205, 206]

Australia

In March 2019, the Australian Government released its "Responsible Release Principles for Cyber Security Vulnerabilities," which outlines the process used by the Australian Signals Directorate[207] to determine whether vulnerabilities discovered should be disclosed to the vendor for patching or retained for offensive means.[208]

The process outlined in Australia's "Responsible Release Principles for Cyber Security Vulnerabilities" is very similar to that of the current VEP, and is overseen by the Australian Signals Directorate: once a vulnerability is discovered, it goes through an assessment to see if there is critical intelligence that would justify retaining the vulnerability:

1. If not, then the vulnerability is disclosed for patching and is cited in an annual report to the Inspector-General of Intelligence and Security, as well as in an annual report to the Minister of Defence.
2. If so, the vulnerability is retained and will be reassessed every twelve months until it is disclosed.

The vulnerability assessment process – led by an "Equity Steering Group" composed of technical experts – also closely resembles that of the VEP, including an initial determination phase and pre-determined processes with how to reconcile disagreements. One key distinction from the US' VEP, however, is that the "Responsible Release Principles for Cyber Security

---

[205] Aldrich & Kasuku, 2012.

[206] For an in-depth review into this topic, including the evolution and role of national intelligence during the post-Cold War, I recommend reading Michael Herman's *Intelligence Power In Peace and War*, 1996.

[207] The Australian Signals Directorate is a member of Australia's national security community and is tasked with defending the national interests of Australia from global threats, working across the full spectrum of intelligence, cyber security, and offensive operations in support of the Australian Government and Australian Defence Forces. (Australian Signals Directorate, n.d.a.)

[208] Australian Signals Directorate, n.d.a.

Vulnerabilities" is a pro-disclosure-oriented policy, stating that the "[Australian Signals Directorate's] starting position is simple: when we find a weakness, we disclose it."[209]

Canada

The Canadian Government's "Equities Management Framework" – published in March 2019 – is managed by the Communications Security Establishment (Canada's national cryptologic agency). This framework is also very similar to that of the US' VEP, and "provides a standardized decision-making process in which [Communications Security Establishment] experts consider all available information to responsibly manage equities associated with an identified vulnerability in an information system or technology."[210] This process is composed of a Technical Panel (which assesses the vulnerabilities brought forward and provides an initial recommendation) and an Equities Review Board (which reviews the Technical Panel's assessments and confers on a final decision) that both meet regularly, and also has a pre-determined processes to reconcile disagreements. Similar to Australia's process, Canada's "Equities Management Framework" also reassesses each retained vulnerability every twelve months until they are disclosed. According to a Communications Security Establishment spokesperson Ryan Foreman, the "Equities Management Framework" (or something very similar) had been "a longstanding assessment process" used by the Canadian Government "to review and assess software vulnerabilities" prior to its March 2019 publication.[211, 212]

Canada's "Equities Management Framework" has received similar criticisms to that of the VEP, including skepticism around whether the Communications Security Establishment – an intelligence agency – is the proper entity to lead such an effort given that their offensive and defensive units with opposing goals could potentially influence the final disclosure or retention decisions.[213]

United Kingdom

The United Kingdom published its federal level vulnerability equities process (referred to as the "Equities Process") in November 2018, which falls under the jurisdiction of the Government Communications Headquarters (the United Kingdom's signals intelligence and information assurance organization – similar to the NSA, CSE, and ASD).[214, 215] This Equities Process is very

---

[209] Australian Signals Directorate, n.d.a.

[210] Government of Canada, 2019.

[211] Braga, 2017.

[212] Charlet et al., 2017.

[213] Braga, 2017.

[214] Levy, 2018.

[215] National Cyber Security Centre, 2018b.

similar to that of the US VEP.[216] When a vulnerability is submitted it goes for review by an Equities Technical Panel (composed of subject matter experts from the United Kingdom's intelligence community, including the National Cyber Security Centre) which make an initial determination on whether the vulnerability should be disclosed or retained. If a consensus for disclosure or retention cannot be reached by the Equities Technical Panel, then it is escalated to the Government Communications Headquarters Equity Board (composed of broader government agency representatives) for a determination – and can be further escalated to the Equities Oversight Committee (chaired by the CEO of the National Cyber Security Centre) if a determination still cannot be reached. As with the US VEP, the United Kingdom's Equities Process lists the decision criteria used during determination deliberations, including equities and exemptions – and goes one step further by stating that any retained vulnerabilities go through a re-evaluation process *at least* every twelve-months until they are disclosed.

Countries on the Path to Developing Publicly Available VEP Policies

At the time of this dissertation's composition (December 2021) Germany, Japan, and Lithuania were actively developing VEP-like policies in the public sphere.

Germany

In June 2018, Germany confirmed that it had not yet installed a formal vulnerabilities review process, but that one was being developed[217] – despite previous reports stating that one such process was expected to be implemented in 2018.[218] A handful of scholars within this cyber policy space believe that Germany's final process will closely resemble that proposed in the Transatlantic Cyber Forum's report titled "Governmental Vulnerability Assessment and Management: Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities."[219, 220] The process workflow very thoroughly outlined in this 2018 report appears to be quite similar to the current US VEP, complete with an Executive Secretariat, a vulnerability assessment that includes technical subject matter experts, and an equities review.[221] Similar to the Australian and Canadian models, this proposed process also includes a reassessment every twelve months of each retained vulnerability until they are disclosed.

There is one item in particular from the process proposed by the Transatlantic Cyber Forum's report that is worth highlighting: given that a majority of the stakeholders involved in this process may be from the intelligence community and may be biased towards vulnerability

---

[216] Government Communications Headquarters, 2018.

[217] Council on Foreign Relations, 2018

[218] Schaake et al., 2018.

[219] Herpig & Schwartz, 2019.

[220] Bradford Franklin, 2019.

[221] Herpig, 2018.

retention, the assessment process only requires a 15% minority of those in favor of "disclosure" to trigger a vulnerability disclosure. If this exact process is in fact adopted by Germany, this would be the only policy of its kind that provides actual values associated with the process to the public.

Japan

Although Japan has an extensive vulnerabilities disclosure process that incorporates both the public and private sectors, it is unclear to what degree vulnerability "disclosure" versus "retention" is weighed. The overall vulnerability disclosure process itself is called the "Information Security Early Warning Partnership Guideline" and was originally established in 2004 (although it was last updated in 2017) by the Ministry of Economy, Trade, and Industry when they issued the "Standards for Handling Software Vulnerability Information and Others."[222, 223] When a vulnerability is discovered (regardless of origin), it is submitted to the Information-technology Promotion Agency (a policy implementation agency under the jurisdiction of the Ministry of Economy, Trade, and Industry) for analysis, and is then forwarded to the respective vendor for remediation, as well as to the Japan Computer Emergency Response Team Coordination Center (an independent non-profit organization) for publication; all associated security alerts and vulnerability notes are published on the Japan Computer Emergency Response Team Coordination Center website.[224, 225] The publication of these vulnerabilities does not occur until the vendor has the opportunity to provide a patch. Unfortunately, though, there is no public information on how the Information-technology Promotion Agency conducts their vulnerability assessment, what is included in that assessment, what entities are involved in the process, and whether or not "disclosure versus retention" is considered.

Lithuania

Lithuania's Ministry of National Defence has drafted an amendment to their *Law on Cyber Security of the Republic of Lithuania* that will provide the legal basis necessary to begin the formal development of a national level vulnerabilities equities process.[226] As of September 2020, the Ministry of National Defence was planning a forum to facilitate an initial dialogue between potential stakeholders of the national level process (including law enforcement) regarding the proposed legal regulations, possible challenges, and to clarify any vagueness.[227]

---

[222] Information-technology Promotion Agency, n.d.a.

[223] Information-technology Promotion Agency, n.d.b.

[224] JPCERTCC, n.d.a.

[225] JPCERTCC, n.d.b.

[226] Schaake et al., 2018.

[227] Ministry Of National Defence Republic Of Lithuania, 2020.

Coordinated Vulnerability Disclosure Programs

This research has highlighted that very few countries have a publicly available national-level vulnerabilities equities process in place to determine whether a newly discovered vulnerability should be disclosed to vendors for patching or retained by the government for future use. With that said, though, a surprising number of countries do have a coordinated vulnerability disclosure (CVD) program in place – or are actively working towards one – in order to encourage private sector entities (including educational and research institutions) to promptly inform the government of vulnerabilities discovered across government systems or other critical systems. Some of these countries include Belgium (which has a CVD initiative through the Global Forum on Cyber Expertise)[228], Finland (which published a Vulnerability Coordination Policy, overseen by the National Cyber Security Center Finland [NCSC-FI])[229], the Former Yugoslav Republic of Macedonia (which has a general policy on information disclosure that is publicly available in the local Macedonian language)[230], France (which has ongoing development efforts with the establishment of Art. 47 of the Law for a Digital Republic, led by Agence Nationale de la Sécurité des Systèmes d'Information [ANSSI])[231], Italy (which is working on harmonizing their CVD initiative with current national laws, led by the Digital Transformation Team)[232], Luxembourg (which has a Responsible Vulnerability Disclosure program, led by Computer Incident Response Center Luxembourg [CIRCL])[233], Latvia (which has a Responsible Disclosure Policy overseen by the government's CERT, but is working towards developing a more robust program)[234], the Netherlands (which implemented a CVD program back in 2013, and which has been very successful in incentivizing private organizations to actively participate in the program)[235], Romania (which is working towards a CVD program as part of the Global Forum on Cyber Expertise (GFCE) initiative, supported by the Ministry of Foreign Affairs)[236], Singapore (which has a very robust CVD program in place for their private sector)[237, 238], and the United States (which has a CVD process overseen by DHS' Cybersecurity & Infrastructure

---

[228] Center for Cyber Security, n.d.

[229] Schaake et al., 2018.

[230] Schaake et al., 2018.

[231] Agence Nationale de la Sécurité des Systèmes d'Information, n.d.

[232] Digital Transformation Team, n.d.

[233] Computer Incident Response Center, n.d.

[234] Informācijas technoloģiju drošības incidentu novēršanas institūcijas, 2016.

[235] National Cyber Security Centre, 2018a.

[236] European Institute of Romania, 2018.

[237] Government Technology Agency, n.d.

[238] Cyber Security Agency of Singapore, 2016.

Security Agency [CISA]).[239] The United States also recently launched their Vulnerability Disclosure Policy (VDP) Platform[240] managed by CISA which provides a centrally managed website that agencies can leverage as the primary point of entry for intaking, triaging, and routing vulnerabilities discovered within their own websites by researchers. It is also worth noting here that US Cyber Command has used the platform VirusTotal (a publicly available platform for analyzing files and URLs for malicious content) to notify the international cybersecurity community of unclassified malware samples since 2018.[241, 242]

This type of CVD or VDP program, however, is outside the scope of this research.

Chapter Conclusion

In this chapter I traced the evolution of the VEP, beginning with NSPD-54 and the CNCI in 2008, through its original iteration as the "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process" in 2010, and ending with the release of the updated charter in 2017. As part of this effort, I also looked at how the structures of these documents changed over time, along with a review of publicly available criticisms; this provided more understanding into how the public's view of these documents also changed over time – approving of the increased transparency, but still desiring codification to improve enforceability, the closing of perceived loopholes created by exempting vulnerabilities associated with NDAs or partner agreements from review, the replacement of the NSA as Executive Secretariat, and a more robust consideration of consumer and industry equities. Industry stakeholders echoed this particular concern, claiming that their lack of involvement in the VEP exposes both the public and service providers to unnecessarily risk.

I then performed a review for any proposed legislation related to the VEP to see how many bills made it to Congress for consideration, what their key objectives were, and how many (if any) made it to codification. My review uncovered three related efforts: the PATCH Act and the Cyber Vulnerability Disclosure Reporting Act (both from 2017) which did not make it to codification, and 50 U.S. Code § 3316a ("Reports on intelligence community participation in vulnerabilities equities process of Federal Government") of 2019 which did; 50 U.S. Code § 3316a is meant to codify the annual reporting requirement of the VEP (including the associated process and criteria).

To add perspective to my research on the US VEP, I reviewed how other countries are formally addressing the topic of equities-based vulnerability review at the national level. From this review, I found that only three countries (aside from the United States) have a publicly

---

[239] Cybersecurity & Infrastructure Security Agency, n.d.

[240] Cybersecurity & Infrastructure Security Agency, 2021b.

[241] CYBERCOM_Malware_Alert, n.d.

[242] Cimpanu, 2018.

available VEP-like policy in place, all of which are of the Anglosphere: Australia, Canada, and the United Kingdom. Several other countries claim to be developing a VEP-like policy or have a cyber vulnerability disclosure program in place (although this is outside the scope of this research).

After analyzing my findings from this chapter, it is clear that there are two main areas where new research would bring additional value to continuing the informed evolution of a now-public VEP policy. The first area where additional research is needed is centered around the process itself. The most glaring gap is the fact that the current VEP charter – although a step in the right direction – is not enforceable; without an appropriate accountability mechanism in place, the charter merely provides a policy stance without obligating compliance. This leads us to ask what type of enforceability mechanism would be best to implement (e.g., a statute versus an Executive Order)? In this section we are also left with questions regarding the use of NDAs and partner agreements. Critics of the current VEP charter were very vocal about this being a potential loophole (although one could argue that not having an enforceable VEP to begin with is perhaps the largest loophole of all), but there is no public information on whether these means of vulnerability acquisition are in fact leveraged as "loopholes," nor do we know how often these two exemptions actually apply during the regular course of operations. We should be able to locate this type of information in the unclassified annual reports identified in the charter (and most certainly within the classified versions), but again we are faced with a knowledge gap since I was unable to locate any unclassified annual reports related to VEP adjudications. And finally, another key public concern that belongs in this category is the desire to have a more neutral entity replace the NSA as Executive Secretariat. While many within the media and digital advocacy groups suggested DHS as an appropriate replacement, it is unclear whether DHS would in fact be an unbiased replacement, nor do we have conclusive evidence that NSA is in fact a biased Executive Secretariat to begin with, or if the disapproval was perhaps more of a byproduct of the general mistrust that had already been brewing as a result of the Snowden and Heartbleed incidents.

The second area where additional research is needed is focused around the conversation on equities. One of the first equities-related concerns pointed out in the public critiques of the current charter is that its decision-making body (the ERB) is primarily composed of intelligence or law enforcement entities; this suggests that consumer and industry stakeholder representation is almost entirely absent, or that the US Government believes that those equities are adequately reflected through the equities of intelligence and law enforcement stakeholders. While the meager equities considerations for industry – along with the notable absence of an equities consideration section for consumers or general citizenry – on the surface appears to support this claim of a gap in representation, again we have no publicly available information on whether or not the actual ERB discussions that unfold adequately represent the equities of these stakeholders. Along the same lines, it is unclear why international-oriented equities appear to be given little consideration, particularly when acknowledging that no other countries outside of

Five Eyes have a similar national level program (or at least one that is publicly available). In this section we also face questions regarding why private sector involvement is glaringly absent from the VEP charter, particularly due to the emphasis Congress has placed on the importance of including industry in national level cyber security initiatives given industry's majority control over US cyber infrastructure.[243] And finally, information around how the VEP charter may or may not be expected to accommodate the government's evolving use of technology and vulnerabilities (e.g., the FBI's use of the Mozilla vulnerability in Operation Pacifier) is an area of knowledge that is lacking and would provide value for future conversations around the public's expectation of cyber related public policies.

[243] U.S. Senate Committee on Homeland Security & Governmental Affairs, 2008.

Chapter 2: Qualitative Research & Analysis of the VEP

As we saw in Chapter 1, the information currently available to the public is insufficient to answer critical questions about the design of the Vulnerabilities Equities Process' (VEP) charter. To begin developing any new hypotheses or drawing meaningful conclusions, new data is required. At the end of Chapter 1, I identified the two key areas[244] where this data generation should be focused. The first area is on new information related to the process itself, particularly regarding the appropriate mechanism to increase enforceability of the VEP, the potential existence and use of loopholes (e.g., Non-Disclosure Agreements [NDAs] and partner agreements), confirming whether the classified and unclassified reports are being generated, and whether there is a more suitable federal entity than the NSA to fulfill the role of Executive Secretariat. The second area to focus the generation of new information on is related to the equities considered during the ERB adjudication process, particularly regarding whether the ERB's current composition (i.e., primarily composed of intelligence or law enforcement entities) imposes bias during the decision-making process, whether consumer and industry stakeholders are adequately represented during these discussions, whether international-oriented equities should be given more consideration, and if the VEP should be expected to accommodate the government's evolving use of technology and vulnerabilities.

Methods Selection

To ensure I used the most appropriate method to generate this new data, I performed a review of research approaches spanning both the quantitative and qualitative spectrums. To begin, I looked at the methodological assumptions, objectives, and sampling guidelines of both the quantitative and qualitative approaches on a general level.

Quantitative research is generally defined as research that uses mathematically-based methods (especially statistics) to analyze numerical data in order to explain a phenomena of interest.[245, 246, 247] It is rooted in objectivist epistemology[248, 249] – the idea that there exists a "true" reality independent of individual perceptions – and seeks to explain the relationship between

[244] Please refer to Chapter 1 to review the research that led to the identification of these two areas. A summary can be found in the "Chapter Conclusion" section of Chapter 1.

[245] Yilmaz, 2013.

[246] Gay & Airasian, 2000.

[247] Creswell, 1994.

[248] Yilmaz, 2013.

[249] Firestone, 1987.

phenomena (which it assumes exists in a static state) in terms of generalizable causal effects through "the measurement and analysis of causal relationships between isolated variables within a framework which is value-free, logical, reductionistic, and deterministic, based on a priori theories."[250] Due to the desire to identify the objective reality of a relationship through mathematical means, quantitative approaches generally require a large representative sample and variables which lend themselves to quantification, allowing for generalizability of the findings.[251] Qualitative research, on the other hand, is generally defined as research that leverages an "inductive, interpretive and naturalistic approach to the study of people, cases, phenomena, social situations and processes in their natural settings in order to reveal in descriptive terms the meanings that people attach to their experiences of the world."[252, 253] It is rooted in constructivist epistemology – the idea that reality is dynamic (i.e., there are multiple "realities") and is the result of socially defined frameworks that are "value-laden, flexible, descriptive, holistic, and context sensitive."[254, 255, 256, 257] In contrast to quantitative research, qualitative research almost exclusively leverages purposive sampling strategies to allow for the intentional selection of information-rich cases.[258]

Given these distinctions, employing a qualitative approach to my research will provide more data-rich findings for my particular needs than if I employed a quantitative approach. I arrived at this conclusion for three key reasons. First, the questions I will need to ask (given the key areas of research outlined above in the "Introduction") are subjective in nature and strive to develop a more robust contextual understanding of the VEP through individual experiences and perspectives, which already implies the acknowledgement of multiple realities across the individuals responding and the context of their relationship with the VEP; the generalizable objective of quantitative approaches limits the ability to capture this level of insight into individual experiences.[259] Second, nearly every aspect of the VEP – including the final decisions themselves – are contextual and dynamic, whereas a quantitative approach assumes a static state. And third, the sampling pool available to me is incredibly small, which is a byproduct of the restrictive nature of who has historically had access to and interactions the VEP; this means that I

[250] Yilmaz, 2013.

[251] Gelo et al., 2008.

[252] Yilmaz, 2013.

[253] Brewer & Miller, 2003.

[254] Yilmaz, 2013.

[255] Gelo et al., 2008.

[256] Denzin & Lincoln, 1994.

[257] Firestone, 1987.

[258] Gelo et al., 2008.

[259] Yilmaz, 2013.

will need to do purposive sampling in order to (1) achieve a large enough sample size, and (2) ensure that my sample is also inclusive of as many perspectives of possible.

Proceeding with a qualitative research approach, I decide to root my research in thematic analysis for reasons outline below. Thematic analysis is a type of inductive analysis of qualitative data that can be achieved through multiple analytical techniques, but whose aim is to systematically generate theories rooted in the identification of patterns of meaning (or "themes") across a given set of qualitative data.[260, 261, 262] Thematic analysis is an approach that is widely used across different fields – often combined with quantitative methods as well for form a mixed methods approach – but is particularly used within public policy as it relates to equity, social work, education, and health (including both physical and mental health).[263, 264] The benefits of leveraging a thematic analysis method is that – if performed rigorously – it can yield trustworthy and insightful findings,[265] lends itself particularly well to examining the perspectives of different participants,[266] and is very useful for uncovering unanticipated insights.[267] Distinct from methods found under a quantitative approach which rely on demonstrating reliability and validity of their findings, the quality of a study employing thematic analysis is assessed in terms of the study's "trustworthiness," [268] which is demonstrated by fulfilling the four criteria of *dependability* (is the research process is logical, traceable, clearly documented), *confirmability* (can the results be confirmed or corroborated by other participants), *credibility* (are the findings believable), and *transferability* (are the results generalizable for a similar context).[269] Given the level of documentation I maintained throughout my qualitative research, along with the high level of corroboration across interviews on the themes that emerged, I believe I have successfully demonstrated that my findings are trustworthy.

There are other means of qualitative data analysis, including content analysis, grounded theory, interpretive phenomenological analysis, narrative analysis, and discourse analysis, but the limitations of these other methods made them less ideal to leverage when compared to thematic

---

[260] Terry et al., 2017.

[261] Vaismoradi, 2016.

[262] Guest et al., 2014.

[263] Castleberry & Nolan, 2018.

[264] Ward et al., 2017.

[265] Braun & Clarke, 2006.

[266] King, 2004.

[267] Nowell et al., 2017.

[268] Lincoln & Guba, 1985.

[269] *Transferability*, although a dimension of trustworthiness in qualitative studies, is generally viewed as being the responsibility of the researcher doing the transferring or generalizing to their case or study; this researcher is responsible for assessing the context of their study and making a value judgement on whether it is sensible to transfer the results from the original study into their study.

analysis. For example, content analysis[270] – which evaluates content (e.g., images, text) for patterns – is known to not be particularly good at picking up nuances that were not accounted for from the onset of a study; in the case of my research, nuances in my participants' perspectives of the VEP are very important in uncovering new insights. Grounded theory[271] – which takes an overarching question and waits for patterns to emerge, which are then tested on new sample groups – requires a researcher to step into a study with little structural boundaries in order to be guided completely by data as it unfolds; while this in and of itself is not a limitation, grounded theory also requires the researcher to "test" any new theory that may be emerging from the data on new samples of participants; given the exceptionally small sample pool I will have available, I do not believe that I will be able to achieve reliable or verifiable results though this method. Interpretative phenomenological analysis[272] is not congruent with my overall objective – which, when generalized, is to learn more about the VEP through differing perspectives – because it focuses on an event or experience that happened to a participant. Similarly, narrative analysis[273] (which analyzes individual story telling for their deeper meanings) and discourse analysis[274] (which analyzes communications within their social context) are also not congruent with my over overall objective because. Looking back at thematic analysis, the main limitation associated with this method is its flexibility, which can lead to inconsistencies and a lack of coherence if an epistemological position (e.g., objectivist versus constructivist epistemology) is not explicitly identified from the beginning to underpin the study.[275]

A thematic analysis itself can be approached in either a confirmatory or exploratory manner. A confirmatory approach is generally used in conjunction with a hypothesis-driven study where a researcher is trying to conclude whether "x people think z about y."[276] In these instances, a researcher will already have predetermined themes, trends, or ideas in mind, and will simply review the final data set for instances of those themes; since these themes are generated ahead of time, a priori, no consideration to potential emergent themes is given. In order to control for bias due to the predetermined hypothesis-driven approach, random sampling will be used. By contrast, an exploratory approach is content-driven, meaning that no themes are determined ahead of time, and will generally ask questions oriented as "What does x person think about y?"[277] Because these studies have general areas of focus – as compared to a much more focused hypothesis-driven confirmatory study – purposive sampling is much more common, allowing

---

[270] Krippendorff, 2018.

[271] Charmaz, 2008.

[272] Eatough & Smith, 2017.

[273] De Fina & Georgakopoulou, 2008.

[274] Van Dijk, 2007.

[275] Nowell et al., 2017.

[276] Guest et al., 2014.

[277] Guest et al., 2014.

researchers to better target information-rich and relevant participants. After data collection, the researcher will carefully review the entire data set multiple times for themes or trends, which will then be used to provide an outline for the follow analysis. Given that I previously identified two general areas of interest where new information is needed about the VEP (please refer back to the "Introduction," or to the "Development of Interview Protocol" section below where these areas are elaborated on), but do not have enough information to begin performing meaningful hypothesis development or testing, employing an exploratory thematic approach is most appropriate.

Now that I have outlined the most appropriate research approach and method for my study – a qualitative research approach employing exploratory thematic analysis – it is time to determine what technique is most appropriate to generate the data. While thematic analysis is most often applied to interview transcripts, it can also be applied to other data sources such as questionnaires with open-ended questions and focus group transcripts. For the purpose of my study, however, I do not believe either of the latter are appropriate. While a questionnaire can promote consistency (both in terms of the questions being asked, as well as the scale or options used for measurement), it also limits the amount of individual perspective and expression that can be captured.[278] In a similar vein, focus groups may be good for deeper examinations of complex issues facilitated by discourse within a group of participants, but they also run the risk of having certain perspectives washed out by stronger personalities – potentially skewing the data.[279] By holding one-on-one interviews, however, I am able to create an environment focused on the views of a specific individual where they are able to express their perspectives and experiences without being influenced by another participant. Furthermore, by leveraging one-on-one interviews, I am able to follow-up on responses to generate additional context around a given statement, as well as have the opportunity to repeat certain insights back to the interviewee to ensure I am accurately capturing and reflecting their responses.

Methodology

This research study leverages a qualitative approach, using interviews as the method of new data generation, and an exploratory thematic analysis as the method of analysis. As discussed in Chapter 1, there is current a very limited amount of available data on the VEP (primarily the VEP charters themselves and a small number of public statements made by government officials). Conducting interviews with VEP subject matter experts and key stakeholders is the most effective method for collecting new data on the VEP process and its implementation.

---

[278] Saldana, 2015.

[279] Bhattacherjee, n.d.

The review of publicly available information related to the VEP (e.g., official government documents, think tank reports, analyses, opinion pieces) performed in Chapter 1 informed the development of the interview protocol.

Development of Interview Protocol

The need to generate new data around two key areas related to the VEP drove the design of the interview protocol: (1) the process itself, and (2) the equities considered during ERB adjudication. These areas were identified during my review of publicly available information in Chapter 1. From that review, we saw that the public discourse surrounding the release of the current VEP charter had resulted in several sets of recommendations and concerns regarding the VEP's process and equities considerations – virtually all of which are based on opinion due to the absence of any official VEP data or comprehensive research studies focused specifically on the VEP. In addition, I also identified a third area that was not explicitly mentioned in the public discourse, but that my review from Chapter 1 supported: the government's evolving use of vulnerabilities, and the role of international equities. The first two areas related to "process" and "equities considerations" are designed to provide perspective on the VEP's current state, while this third area is designed to be more futures-focused.

As such, the interview protocol is divided into three sections with the goal of generating new information around these three key areas. The "process" focused section of the protocol targets topics related to whether implementing an enforceability mechanism for the VEP is viewed necessary by VEP subject matter experts (SMEs) (and what mechanism would be most appropriate); whether the current VEP charter is viewed as having loopholes designed into the process itself (either explicitly as with the categories of vulnerabilities that are exempt from review, or implicitly as with the notable absence of an NDA focused discussion); if any VEP SMEs can confirm whether the classified or unclassified annual reports are being produced; and if the Executive Secretariat role should be filled by the NSA or another entity and why.

Similarly, the "equities consideration" focused section of the protocol targets topics related to whether the ERB's majority intelligence and law enforcement composition are viewed as potentially biasing the adjudication results; and whether consumer and industry equities are viewed as being adequately represented, including the likelihood for patch development/deployment (and if not, how could they be better represented).

And the final section of the protocol is focused on "futures" oriented topics that target views on whether international-oriented equities could or should be given more consideration in the future due to the increasingly degree of global digital interconnectedness; and if or how the VEP should be expected to accommodate the government's evolving use of technology and vulnerabilities in the future.

To provide context to the responses, a question regarding each SMEs relationship with the VEP has been included, as well as an open-ended question at the end which gives the

interviewees an opportunity to bring up any comments or perspectives on the VEP that they view as important but that were not captured in the other protocol questions.

The interview protocol was developed to be used across all interviewees. Given the very small number of individuals familiar with the VEP, the interview could not be beta tested. In lieu of being beta tested, however, the interview protocol was reviewed with a dissertation advisor and determined to take approximately 20 to 30 minutes. In addition, the final interview protocol, all associated procedures (e.g., initial interview outreach, material safeguarding, etc.), and overall study design were submitted to RAND's Human Subjects Protection Committee for review and approval prior to beginning engagement with any VEP SMEs.[280] See Appendix A to view the interview protocol used.

Selection of Participants & Demographics

Given the very small sample pool available, I aimed to interview as many VEP SMEs as possible, and with as much variety as possible (e.g., former government officials, large commercial information technology providers, journalists, etc.). Potential interviewees were initially identified during the literature review phase. Subsequent interviewees were identified via snowball sampling from the initial set of interviewees. When coordinating interviews, each potential interviewee was initially sent a recruitment message via email. These email addresses were gathered from open sources; in a limited number of cases, email addresses were provided to the research by other interviewees. In the cases where the I was unable to locate an email, other means/platforms of contacting the SMEs were used (e.g., LinkedIn, Twitter).

In total, 43 SMEs were identified. Of these 43 SMEs, 32 were sent interview requests, while the remaining 11 were unable to be contacted due to (1) a lack of publicly available contact information, and (2) the inability to identify contact information through a participating SME. Of the 32 SMEs who were sent interview requests, 29 responded – 10 of which indicated they did not wish to participate in the study.[281] Ultimately, 19 VEP SMEs were interviewed across seven industries: Academia / Research, Commercial Information Technology, Federal Government, Intelligence Community, Journalism, Legal, and Military – many of which had interacted with the VEP across the different stages of its evolution, including with the original iteration under the George W. Bush Administration. A large majority of interviewees had experience across more

[280] This study was approved and determined to be a "Category 2—Educational Tests, Survey Procedures, Interview Procedures and Observation of Public Behavior" study by RAND's Human Subjects Protection Committee, and was deemed exempt from any further review. For verification, contact RAND's Human Subjects Protection Committee and reference Study 2021-N0313.

[281] It's worth noting that the majority of the SMEs who declined to participate mentioned that their reason for declining (although a reason was not requested) was that they were actively working within either the intelligence community or government and even though the VEP charter was now unclassified did not feel comfortable commenting on their past experiences, opinions, or perspectives.

than one industry (see Table 1), and had either directly interacted with the VEP in some capacity, or had spent several years researching the VEP in-depth.

Table 1: Interviewee Industry Affiliation

Interviewee	Academia / Research	Commercial Information Technology	Federal Government	Intelligence Community	Journalism	Legal	Military
#1	X		X				
#2	X						
#3			X				
#4					X		
#5	X					X	
#6	X						
#7		X	X				
#8	X						
#9	X		X				
#10	X					X	
#11	X			X			
#12		X	X				
#13	X						X
#14		X		X			
#15			X				
#16	X		X				
#17	X						
#18	X		X				
#19	X			X			X
TOTAL	**13**	**3**	**8**	**3**	**1**	**2**	**2**

Conducting the Interviews

All interviews were conducted over the phone. Each interview was conducted on a one-on-one basis – with only the interviewee and myself present. As previously mentioned, the interviews consisted of a semi-structured format following a pre-developed interview protocol (see Appendix A). This method allowed me to follow-up on specific perspectives expressed by an interviewee, and also allowed me to repeat summarized versions back to confirm that my understanding and notes accurately reflected their perspective.

The interviews were not recorded, but transcript-like notes were typed during each interview. The interview notes were then input into a spreadsheet – each row representing a unique interviewee, and each column representing a specific question from the interview protocol; any

information that could be used to identify the interviewees was excluded from the spreadsheet. Once all interviews had been conducted, the aggregated responses were examined several times for insights in the form of emergent themes. After these themes were identified, the responses were reviewed once again and were assigned themes where applicable (see the "Interview Results" section for the list of themes identified). A tally of how many interviewees expressed each theme was later calculated in order to provide percentages for the analysis and "Interview Results" write up; an interviewee could only be counted once per theme (e.g., even if an interviewee expressed a particular theme several times, they were only counted once for the percentage calculation).

Interview Results & Limitations

The exploratory thematic analysis of the interview data resulted in the identification of twelve key themes: (1) an ERB member's agency affiliation does in fact influence their "disclosure vs. retention" vote; (2) the unclassified annual VEP reports are not being published, although classified reports to Congress appear to be happening; (3) additional formalization of the VEP is desired to make its enforcement possible; (4) the NSA does seem to be the most appropriate federal entity to hold the role of Executive Secretariat due to their technical abilities and intelligence function; (5) the majority intelligence and law enforcement representation currently present within the ERB appears to potentially be influence adjudication outcomes; (6) the equities of consumer and industry stakeholders should be better represented during ERB discussions, but there is no clear consensus on how to achieve that goal; (7) the ERB does take a vendor's potential response to a disclosure decision into account – mostly to assess how likely the vendor is to develop a patch, how much lead time they will require to develop a patch, and how likely it is that the patch's application will negatively impact the vendor's revenue stream;[282] (8) there are many more steps that industry can be taking to better protect their consumers from vulnerabilities; (9) even as the government's use of technology and vulnerabilities continue to evolve, the VEP should remain focused solely on the adjudicating of zero-day software vulnerabilities; (10) more inclusion of an international perspective during the adjudication process would be valuable, but not through the addition of new ERB member; (11) the VEP could be used to support the development of a global set of equities to drive global norms around vulnerability exploitation; and, (12) the VEP also serves as a guide for ERB members on how to make ethical decisions around the retention or disclosure of software vulnerabilities. Each of these themes and their associated analysis is outlined in the following sections.

[282] This is viewed as a proxy for "likelihood to develop the patch;" interviewees felt that if a patch is likely to negatively impacts functionality, vendors are less likely to want to develop the patch because it may negatively impact their revenue stream. Please refer to the "A Vendor's Response To A Dissemination Decision Is Considered By The ERB" section for a comprehensive discussion of this theme.

The research findings have two general limitations: the sample size and diversity. The sample size itself (n = 19) may appear small, but given the relatively small number of individuals who are VEP SMEs (this research identified roughly 43 in total), the small sample size was expected. As such, a larger sample size may have uncovered additional insights, but I do not believe those insights would have significantly altered the findings reached. The emergence of new themes dropped off sharply after the second interview, and theme saturation was achieved after the thirteenth interviewee (meaning that no new themes emerged after the thirteenth participant was interviewed), with the majority of themes being identified by the seventh interview (see Figure 1). The threshold for meeting saturation in qualitative research has been consistently debated and researched over the past twenty years.[283] Morgan et al. – widely regarded for their landmark study on saturation in qualitative research – found that the majority of new themes emerged within the first five to six interviews, and that little new information was gained as the sample size approached twenty, with 92% of all new themes being identified by the tenth interview.[284] Guest et al.,[285] Francis et al.,[286] and Namey et al.[287] all reported similar findings, with the majority of themes being identified within the first six interviews, and 92% of themes being identified by the twelfth interview. Hagaman and Wutich[288] found that they regularly achieved theme saturation within less than sixteen interviews. I believe that my findings of the majority of themes being identified by the seventh interview is consistent with the literature, and that I was able to reach a high level of saturation through my total interviews conducted.

Diversity in the industry types represented by the interviewees was another limitation encountered in this section of my study. Academia / Research Institutions (n = 13) and Federal Government (n = 8) were the most represented in the study, with Commercial Information Technology (n = 3), Intelligence Community (n = 3), Legal (n = 2), Military (n = 2), and Journalism (n = 1) the least represented.[289] Although several attempts were made to increase the number of interviewees for these less-represented groups, I was unable to do so within the timeline of this study. As such, the research findings may omit insights specific to these populations.

---

[283] Guest et al., 2020.

[284] Morgan et al., 2002.

[285] Guest et al., 2006.

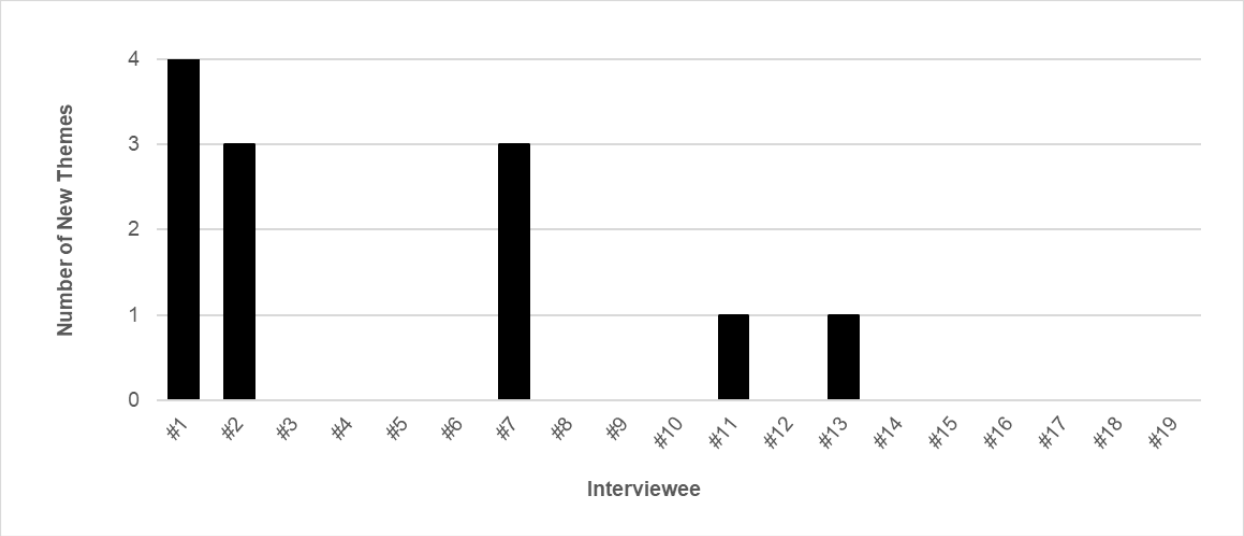
[286] Francis et al., 2010.

[287] Namey et al., 2016.

[288] Hagaman and Wutich, 2017.

[289] It is worth noting that Academia / Research Institutions and Government are the two populations most likely to be involved in in-depth interactions with the VEP, so it is understandable that these two populations would have more VEP SMEs and, therefore, more representation in the interviews.

Figure 1. Number of New Themes That Emerged During Interviews (by Interviewee)



Agency Affiliation Influences "Disclose vs. Retain" Decisions

The majority of interviewees (~90%) believed that a voting ERB member's agency affiliation did influence their desire to either retain or disclose a software vulnerability, and that this influence was directly linked to the mission of the agency which the ERB member represented (e.g., CIA, DoJ). Interviewees, however, did not necessarily viewed this as a negative trait, and generally expressed understanding and support for ERB members advocating in the best interest of their respective agency:

- "Looking at their agency missions and backgrounds, it would make sense that they don't vote to disclose every time."
- "Of course. It makes sense that they would lean towards what the mission of their respective agency is."

A common theme among interviewees, though, was uncertainty around whether these agency representatives were overly influenced to the point where they would knowingly disregard information that would support disclosure to retain access to a software vulnerability.

Unclassified Annual VEP Reports Are Not Being Published

These interviews confirmed that unclassified annual reports outlining metrics of vulnerabilities and decisions made through the VEP have not materialized, even though the most recent VEP charter commits to doing so:

- "They are not out there."
- "I have not been able to locate any unclassified reports."
- "No, the unclassified reports do not exist, but they should, and that's something I think this administration should do."

It is believed, though, that classified versions are being produced and provided to Congress:

- "Congress has said that the House and Senate Intel Committees might be getting reports, but are protective of the process."
- "I hear that there are reports being sent to [Congress]."

Enforceability of the VEP Is Desired

Even though the newest publicly released VEP charter has drastically increased transparency, a majority of interviewees (~85%) supported the addition of an enforceability mechanism into the VEP, identifying this lack of enforceability as a loophole. This support is rooted in four key reasons (listed in order of the frequency they were mentioned):

1. Enforceability is necessary to ensure the VEP's longevity:
    - "[Enforceability] is needed to make sure it doesn't fall apart again. There was a gap from 2008 to about 2012 or 2013 where it was dormant."
    - "[Enforceability] would help make sure it doesn't fall dormant, and that's there's regular thought towards oversight."
2. Enforceability would further promote transparency:
    - "[Enforceability] would allow us to know when changes to the process are made. Since it's just policy right now, we have no way of knowing if any changes have been made."
    - "The VEP is intended to arbitrate the equities of a known or potential vulnerability by the IC on behalf of the civilian population… whether or not they are actually doing that, we don't know."
    - "When things are not enforced, they are just policy and can be changed."
3. Enforcement sets the basis for accountability, which would allow for both internal and external oversight:
    - "Right now people can avoid the VEP entirely if they chose to, but if it was codified then we now have an enforceable mechanism in place and can begin to identify potential loopholes."
    - "Even though the charter has been made public, there still is no requirement to go through it. An enforcement mechanism would help with this."
    - "Since it has no legal standing, there's no requirement to comply with the charter. The fact that the unclassified annual material has not materialized is good evidence that codification is necessary."
    - "With codification, Congress can pressure the Executive branch to actually produce those reports. This is intelligence collection for the President; the IC works for the President... and it's the President's call to choose to put these speedbumps in place."
4. Enforcement and accountability would promote public confidence in the process:
    - "By enforcing [the VEP] you bring oversight and enforcement into the picture, which helps the public believe the process really exists."

Only ~25% of the interviewees, however, preferred codifying the VEP into statue. The majority believed that enforcement through either an Executive Order or a National Security Memo would

be ideal, providing a means of accountability while maintaining flexibility to be able to adapt to threats as they evolve:

- "The cyber domain is rapidly changing, and when you have a rapidly changing domain and need to make strategic decisions, [a statute] is a mistake. We need something that can change to fit our needs."
- "We might not want a statute because that may be too rigid. An EO or security memo is the best way to go."
- "There are alternatives to codification, like the issuing of an EO or a national security memo by the President."

The interviewees who did not support the addition of an enforceability mechanism into the VEP cited two key reasons (listed in order of the frequency they were mentioned):

1. The belief that it would impose unneeded stringency over the VEP that would make the process more difficult to execute and adapt to emerging needs:
    - "Codification is not desirable. These are classic executive branch policy decisions. If there truly was an important vulnerability that came to light, it would be elevated up the appropriate chain for review, regardless of codification. […] Even if you codify it, if it's too cumbersome, people won't listen to it; people will find a workaround for cumbersome processes."
    - "Too much statutory structuring of the exec branch is not useful; it reduces flexibility, it reduces the President's ability to manage the executive branch with flexibility. Not everything benefits from further structure."
    - "The VEP currently works as-is, no need codifying it as that will just make it more difficult to undue or change in the future if our needs change. Flexibility is key when dealing in the cyber domain."
2. The current VEP is not appropriately structured, and the addition of enforcement mechanisms would only make it more difficult to amend:
    - "Codifying the current VEP means you think we already have a good solution, and I'm not convinced that the current VEP is what we want. Codifying restricts your options and makes it more difficult in the future."

NSA Should Continue to Hold the Executive Secretariat Role

The majority of interviewees (~80%) believed that the NSA is the appropriate entity to hold the role of Executive Secretariat, citing that they had not only performed well in this position in the past, but are arguably the most capable agency of holding the position given the combination of their technical abilities and how informed they are due to their intelligence function – even though the role is administrative in nature, and they do not play any formal role in the decision making process:

- "NSA always ran the VEP process well internally."
- "They are awesome and are a super objective. They upheld the standard, didn't let anyone slack (including other NSA ppl). They took notes and shared all findings, there was a lot of transparency from their end. It is

wholly an administrative function. NSA doesn't have a vote… there never was an issue from my experience."

Very few interviewees viewed this technical ability and intelligence function as a conflict of interest for the position; rather, it was seen as a benefit to help the government make more informed decisions, and many noted that there are mechanisms internal to the NSA (e.g., distribution of tasks, internal function audits) to mitigate conflict of interest concerns. In fact, the potential "conflict of interest" in the NSA holding the Executive Secretariat role was widely characterized as an "optics issue" by the interviewees – suggesting there was no substance to claims of conflict of interest – and that these claims were generally rooted in the potential remaining public distrust in the NSA resulting from past events (e.g., Snowden,[290] Heartbleed[291]).

- "Optics issue. It's a matter of practicality; it needs to be held by someone with enough bodies to actually do the work."
- "I think it's an optics issue, but that shouldn't be the deciding factor. I think it's a reasonable case that the entity that does intel for the US is holding this position… it concerns some people, but that doesn't mean they can't do a good job at it."
- "We really do want the most educated or most informed decision-maker as the Executive Secretariat."

Interviewees that did see the NSA holding the role of Executive Secretariate as problematic, noting that the administrative aspect of the role was not the issue; they were primarily concerned by the NSA's dual role of both supporting cybersecurity as well as exploiting vulnerabilities discovered to further its intelligence mission, and believed that those conflicts could potentially boil over into their role with the VEP:

- "The administrative item is not concerning. What is concerning is that one of their responsibilities is to keep a list of vulnerabilities that have gone through the process; it's a place where – given the NSAs stakes in the matter – they could easily leave a vulnerability off the list. Without some kind of oversight or codification of the VEP, we have no way of accounting for this."
- "It's not the fact that the NSA holds this role that introduces the conflict; it's the fact that the NSA holds both offensive and defensive roles that introduces the conflict. To be fair, there will always be natural, healthy conflict between defensive equities and offensive equities, even when held by different parties. The challenge (at least as your question quite reasonably presumes) is that, as an entity with both roles, the NSA likely comes to the table already having worked that out internally."

[290] Klein et al., 2016.

[291] Please refer to the "Introduction" section of this report for more information on the Heartbleed vulnerability.

When asked which federal level entity would be better suited to perform the role of Executive Secretariat, three options were stated (listed in order of the frequency they were mentioned):

1. The Cybersecurity and Infrastructure Security Agency (CISA) within DHS – although it is worth noting that DHS also holds both law enforcement and national security functions, so whether they would truly be a more neutral party should be researched further (~80% of interviewees who felt the NSA should not hold the Executive Secretariat role stated that CISA would be better fit to hold the role):
    - "Yes, it's a definite conflict of interest. They [NSA] are finding and using these vulnerabilities for information gathering and analysis, so they have a stake in preserving that level of access, so while they are supposed to act as an admin, it can definitely make people doubt because of what their overall mission. So it makes sense to move that function to someone else like CISA or the new Office of the National Cyber Director."
2. The Office of the National Cyber Director within the Executive Office of the President, which was established in 2021 (~10% of interviewees who felt the NSA should not hold the Executive Secretariat role supported this option):
    - "With the establishment of a National Cyber Director, there is some movement going on and we should consider moving the function there. CISA is supposed to be sharing and interacting with industry partners already anyways, so they would be another option I'd consider before leaving it with the NSA."
3. A firewalled portion of the NSA that is specifically in place to perform this function (~10% of interviewees who felt the NSA should not hold the Executive Secretariat role supported this option):
    - "It would be beneficial to the process and its independence and credibility for a fire walled portion of the NSA to handle it. The DHS/CISA or NSC could be another option."

It is worth noting that the majority of interviewees who believed the NSA should remain the Executive Secretariat expressed opposition to another federal entity taking over the role, mainly noting that information gathering entities like the NSA do have a great stake in the safeguarding of these vulnerabilities, and that there is an unnecessary amount of potential risk associated with another entity assuming the role of Executive Secretariat:

- "There are significant security considerations, you're touching on sources and methods for intel gathering, so of course the NSA should be leading it. NSA has to protect these things. If they had to hand everything over to CISA, that would be concerning."
- "You don't want to share your crown jewels and wait to see if others in the VEP will take it away because some random person in this new entity is blabbing about your vulnerabilities."

Majority IC Representation on the ERB May Be Influencing Decision Outcomes

Most of the interviewees (~82%) believed that a majority of the Equities Review Board (ERB) members coming from intelligence community (IC) or law enforcement (LE) entities either "does" or "potentially" poses an issue with respect to the decision-making process; of those interviewees, ~44% believed this majority representation "does" pose an issue, and ~56% believed this majority representation "potentially" poses an issue. As a reminder, the VEP is designed to help VEP participants and the ERB reach a final determination of vulnerabilities under review through a consensus; however, if a consensus cannot be reached, a preliminary determination is via a vote.[292]

Interviewees that believed majority IC and LE representation on the ERB poses an issue cited two key reasons (listed in order of the frequency they were mentioned):

1. The belief that an ERB with majority IC and LE representation does not allow for adequate representation of other relevant equities – consumer and industry equities being noted in particular (this was the most often referenced reason):
    - "There is a deficit in consumer or public interest in that there may be risks in not disclosing that are not known to the parties involved in the ERB decision-making process. They might miss scenarios or other compounding factors from those communities, which creates an equities imbalance."
    - "There needs to be better representation of the private sector and of the public generally. I don't feel Commerce or Treasury are best positioned to represent them, and it's logical to think that might be impacting the decisions being made."
2. That an ERB with majority IC and LE representation introduces bias resulting from a "stick together" mindset:
    - "IC and law enforcement will almost always stick together and outweigh the others."
    - "There is definitely a law enforcement mindset that can get in the way of you seeing or considering other points of view."

Interviewees that believed majority IC and LE representation on the ERB potentially poses an issue cited three key reasons (listed in order of the frequency they were mentioned):

1. If equities have not been prioritized ahead of each ERB meeting (e.g., "we are going to prioritize defensive equities over offensive equities or consumer equities over intelligence gathering equities due to this reason"), then it makes it difficult to know if the appropriate voices are being adequately represented in each meeting – may have an influencing effect on the decision outcomes:

[292] For an in-depth discussion of this portion of the VEP, please refer to section "The Review Process" and "Challenges & Disputes within the VEP" of Chapter 2.

- "The board should be set up in a way that accurately reflects what we as the US believe to important; so if we believe that consumer and civilian equities are important, then we should have adequate representation for them on the ERB."
- "It's more likely that the real issue is that the priorities or hierarchy hasn't been clearly laid out, and because of that the priorities must be re-negotiated each time without all the appropriate voices weighing in. If, during the process, the policy clearly stated that defensive needs take priority, then the burden is on the offensive community to justify non-release. On the other hand, if the policy clearly stated that offensive needs are prioritized, then the defensive community has the higher burden, and that might benefit from additional civilian input. If there's not defined hierarchy of priorities ahead of time though, how do we know which interests are represented and to what extent?"

2. If the current ERB members through their majority IC and LE representation do not adequately represent both DoD and non-DoD equities, then the resulting imbalance may have an influencing effect on the decision outcomes:
    - "A good question is 'Do we have the right people representing non-DoD equities?' Is Commerce adequately representing the equities of the American public? If not, then we don't have the right mix of people on that board."
3. The approach used to reach a dissemination or retention decision highly influences whether or not majority IC and LE representation on the ERB poses an issue. If a consensus approach is used, then the potential impact is limited – but if a majority vote approach is used, then there is a much greater probability that the majority IC and LE presence on the ERB is having an influencing effect on the decision outcomes:
    - "When I sat on the ERB, our method was not to take a vote, but to get to a consensus, and if you're doing a consensus then you don't need to worry about weighing certain members' decisions to make sure everything is equitable. Voting in this context is very hard to do in a truly equitable way."

Those interviewees that did not believe majority IC and LE representation on the ERB adversely influenced decision outcomes cited that it is the duty of those agency representatives sitting on the ERB to advocate for the interest of their agencies – not for the interests of others – and because of that there is no inherent issue present:

- "I would hope that each board member would represent their agency and what their agency needs. If the FBI is trying to use a technique to help their most important cases, then I would expect their representative to absolutely advocate to retain that vulnerability."
- "The history of the VEP is realizing that a lot of the research on these vulnerabilities and their discovery is being done by agencies whose mission is to gather intel or exploit for operations."

They also noted, however, that even though the ERB representatives had no obligation to advocate for interests outside of their own, that all ERB discussions were in fact healthy debates that were inclusive of all equities (including consumer and industry equities).

- "When I was in these meetings, those debates were very healthy and included consumer and industry equities that were represented by Commerce and DHS."
- "They don't need to stick to their own entity's views; they can advocate for the broader good if they chose to."

Consumer & Industry Equities Should Be Better Represented, but "How" Is Unclear

The majority of interviewees (~73%) believed that consumer and industry equities could and should be better represented during ERB discussions:

- "There needs to be better representation of the private sector and of the public generally. I don't feel Commerce or Treasury are best positioned to represent them."
- "Industry and consumers are definitely not well-represented, and there are lots of opportunities to include them."
- "It would be good to have an industry or consumer rep just to make sure we're taking all equities into account."

The remaining ~27% of interviewees believed that consumer and industry equities were already adequately represented during ERB discussions and questioned what additional value would be gained from dedicating more time and resources to these two stakeholders in particular:

- "When I was in these meetings, those debates were very healthy and included consumer and industry equities that were represented by Commerce and DHS."
- "This is purely something for the executive branch, so why would we need additional industry representation? I just don't see us solving any problems by having more private sector representation."
- "ERB can reach out, but they don't always want to do that."

The interviews highlighted five potential formats for increasing consumer and industry representation across the entire VEP – not solely during ERB meetings (listed in order of the frequency they were mentioned):

1. **Leverage the Existing ISACs for Consumer / Industry Representation:** This format is very similar to the previous format, but leverages the existing national Information Sharing and Analysis Centers (ISACs) as points of consumer and industry representation. Potential benefits to this approach include: ISACs are aligned with specific private sector industries (including critical infrastructure) meaning that specific ISACs can be tapped by the ERB when a relevant vulnerability is being reviewed, and they already hold clearances and can be pulled into classified conversations (effectively removing the "classification" barrier).

- "An ISAC as a rep at the table is a good idea, especially since these companies have a big stake in how these vulnerabilities are resolved. The people involved usually have a clearance, so this would at least get us around the classification issue."
- "Utilizing the ISACs is a good option that I think should be studied a bit more."
- "Probably better off using one of the existing ISACs because then we won't have parallel things going on. That was one reason for the argument of moving the VEP into DHS because they are already in contact with all the ISACs and have many more ties to different industries."

2. **Establish a Standing Advisory Panel:** This format entails establishing a standing advisory panel composed of approximately eight to twelve public interest stakeholders that would be able to receive and answer specific questions handed down to them by the ERB (including broader trend-related questions). This approach would enable the sanitization of classified information out of the questions themselves, creating an artificial wall between the advisory panel and the classified components being discussed within the ERB. Some interviewees, however, believed that even if all classified information was removed from the questions submitted to the advisory panel, the panel members would try to identify the vulnerability and impacted systems in order to develop a patch – ultimately undermining the VEP's ability to retain certain vulnerabilities if deemed necessary.
    - "If you send a private sector advisory board questions, then they are going to try to reverse engineer those questions in order to find out what new vulnerability has been discovered and who's systems are effected by it."
3. **Solicit Decision Feedback from Cybersecurity Stakeholders:** This format entails generating a list of cybersecurity stakeholders who are well-postured to represent consumer and industry equities. This stakeholder group would receive sanitized information regarding VEP retention vs. disclosure decisions on a rolling basis (e.g., each quarter, this group would receive decision feedback from the vulnerabilities reviewed in the previous quarter, potentially to include general trends on the types of bugs being reviewed as well as trends in adjudication decisions.).
    - "A better way to go about including industry and consumer equities is to have a group of technically qualified stakeholders to review adjudication decision trends. This way they aren't being exposed to any specific information that they could reverse engineer, but are still able to provide high-level feedback regarding potential scenarios that the ERB might not be thinking through."
4. **Dedicated Consumer / Industry ERB Representative:** This format requires having a dedicated consumer and / or industry representative formally added to the ERB. The representative position would be permanent, although the individual in the position would rotate in / out over a predetermined period of time. There are several challenges associated with this format, though, including: overcoming classification issues, determining who fills the role of representative, determining who nominates potential representatives, and how long each person serves as the representatives.

Although an option, most interviewees struggled to see how this format would successfully play out without essentially "giving away" the vulnerabilities being reviewed by the ERB to industry.

- "I don't know how you would ask a subset of industry reps about how a vulnerability might impact things without giving away sensitive information."
- "I think it would be difficult for the private sector to be on the board, because then the cat is kind of already out of the bag and they can go and develop the patch anyways."
- "It wouldn't be great if they were brought into the meetings, especially if it's a vulnerability from their system."

5. **Industry Rep Talks Given to Members of the Intelligence Community:** This format is inverse to the previous four. Instead of having the ERB hand questions down to a designated consumer / industry representative, this format would include industry and consumer representatives (e.g., Cisco, Microsoft) giving talks to members of the intelligence and law enforcement communities (in particular those involved in the VEP) on cybersecurity topics (to include specific hardware / firmware / software components, scenarios, and ongoing vulnerability research) that they view as particularly important to their sector and consumer stakeholders. This format would give the intelligence and law enforcement communities insight into how industry and consumers think about and experience cybersecurity related risks.
    - "Maybe having a person from industry who goes into the IC to talk about how they think about the problem would be a better approach; it eliminates the risk of revealing any classified info, but still informs the IC."

A Vendor's Response to a Dissemination Decision Is Considered by the ERB

The interviewees who had participated in ERB deliberations acknowledged that a vendor's potential reaction to a dissemination decision was considered before a final adjudication was made. Several reasons were given as to why:

1. **How Much Lead Time For Patch Development Is Needed?:** There is always a period of time between when the government notifies a vendor of a vulnerability and when the patch is ready for distribution and application. Interviewees noted that some companies move much faster than others, and that the speed with which a company develops a patch is not always linked to resources (e.g., developing a patch for an ERB-related vulnerability is not always a high priority for every company); there are several other factors that can contribute to patch development time, including the need for independent verification of a vulnerability by the vendor itself, the complexity of the patch's development, and the potential disruption to operations. How long a company will take to develop a patch plays a factor in the ERB's decision on how long they must wait between vendor notification and public dissemination of a vulnerability.

2. **Will A Patch Ever Be Developed?:** Just because a vulnerability is identified and disclosed to a vendor does not guarantee that a patch for that vulnerability will ever be developed. In some instances, the vulnerability impacts a product that a vendor has discontinued and no longer wishes to support, and as a result do not want to invest resources into developing a patch for it. From the ERBs perspective, since the government does not have the authority to compel vendors to develop patches, what is the point of disclosing a vulnerability that most likely will not be patched anyways?
3. **Will Patching The Vulnerability Impact A Vendor's Revenue Stream?**: If patching the disclosed vulnerability will impact the functionality of a feature on a vendor's product, the likelihood of the vendor developing a patch for it decreases sharply ("A vendor will never patch anything that's making them money, full stop.").

A small number of interviewees (~11%) believed that the ERB *should not be* considering a vendor's reaction before making an adjudication decision, citing that the VEP's purpose is to mitigate harm to US national interests on behalf of the *civilian population* – not vendors:

- "The VEP is not a vehicle to improve the security ecosystem on behalf of vendors. It's intended to arbitrate the equities of known or potential vulnerabilities on behalf of the civilian population."
- "Conditioning dissemination decisions on vendors' response is a very dangerous way to approach the VEP and undermines the overall objective of the VEP."
- "The VEP should take whether or not a vendor is going to apply the patch into consideration because it's not related to the core purpose of the VEP."

Industry Can Do More to Better Protect Consumers

There was a general sense across all interviewees (in varying degrees) that private sector companies could be doing more to better protect the consumers of their products and services. These opinions ranged from the idea that vendors should be doing a better job of raising awareness and incentivizing their consumers to have better security practices (to include the increased implementation of automated updating), to the idea that vendors (especially large companies) should be more willing to sacrifice some functionality or profit if it means that their consumers are better protected:

- "Industry fosters insecurity. A great example is that they refuse to put basic add-blockers in place, at everyone's risk. They'll invest in security as long as it doesn't impact their bottom line."

The most commonly expressed opinion was that companies should be investing more into ensuring that any code they are deploying is secure from the beginning:

- "There's a disproportionate amount of emphasis placed on the Government to disclose zero days. If industry has such a big stake in the outcomes and cares so much, then why aren't they investing more resources into ensuring their code is more secure before deploying it and potentially putting their consumers at risk?"

Ultimately, private companies must choose to take actions that better protect their consumers, because the government generally cannot compel a private company to take specific actions.

A handful of interviewees mentioned that they believed the increase in popularity of bug bounty programs may, in some fashion, be feeding the Access-as-a-Service[293] market. If companies chose to not pay "going prices" for zero-day vulnerabilities via a bug bounty program – or chose to not offer a bug bounty program of any kind – these vulnerabilities are likely to then turn up in Access-as-a-Service forums and sold to the highest bidder. While this particular topic is outside the scope of this research, findings from the interviews suggest this is an area where further research is needed.

The VEP Should Remain Focused on Software Vulnerabilities

All interviewees agreed that the VEP should remain focused solely on adjudicating the retention vs. dissemination of zero-day software vulnerabilities, and should not be expanded to include other aspects or topics (e.g., expanding the VEP to include discussions on specific Tactics, Techniques, and Procedures [TTPs] used in conjunction with zero-days):

- "Keep the VEP very focused. It's a very particular matter that is extremely technical, so if you broaden it you would need to raise the level of the discussion to be more general – and this is an area where we want to remain as technical as possible."
- "There are other forums already established here those questions can be better addressed."
- "Things like surveillance oversight or how emergent tech is being used by law enforcement entities is definitely not being adequately addressed in this country… I don't think we have the appropriate frameworks in place yet… but I also don't think that the VEP is the best place for that."

More of an International Perspective in ERB Deliberations May Be Valuable, But Not Through the Addition of an Internationally Focused ERB Member

A majority of interviewees (~64%) believed that more of an international perspective would be beneficial to include in ERB deliberations – and not only to see how certain decisions might impact our allies and partners, but also to consider how they may impact our adversaries as well. This is largely due to the fact that our world has become more technologically integrated and connected through an increasing amount of both public and private systems:

---

[293] The "Access-as-a-Service" market (generally located on the Dark web, but not exclusively) is the provisioning of access to a specific target network, system, or data in exchange for payment of some kind. These services have generally been referred to in the context of hackers or cybercriminals providing access to others of the like, but that trend has been changing. Given the proliferation of technology (and thus, vulnerabilities), an entire legitimate marketplace has popped up around this service model, with companies legally operating and providing their services in the open (such as NSO Group). This, of course, has been met with criticism around the need for regulation of the Access-as-a-service market, and raised questions around the potential for government entities to be fueling this market through their purchasing of vulnerabilities for intelligence gathering or operational purposes. (DeSombre et al., 2021)

- "As our world is becoming increasingly interconnected, attacks are having a broader effect. Take the current supply chain attacks as an example; Solar Winds had a huge impact across a wide number of countries, and we shouldn't expect for this trend to change."
- "Given the nature of vulns in cybersecurity and supply chain attacks, an international perspective is critical as we continue to move forward."
- "I think that in weighing the VEP for the US, you're almost always having to include international equities. There's no way to say 'we'll disclose this only in the US and only patch US equipment' – no, that's not realistic."

Most interviewees did not view the addition of an international representative to the ERB as a plausible option, primarily because there are so many disparate sets of regulations, sensitivities, priorities, and agendas associated with every country when it comes to the cyber domain that it would make moving any vulnerability through the VEP very difficult:

- "I think it might actually create a more restrictive process if we had to navigate all the surveillance regulations and sensitivities of multiple countries rather than just our own."
- "I don't think there is much of a chance for international cooperation. Countries view it as such a big security issue that there's not much willingness to bind oneself in that regard."

The remaining ~36% of interviewees believed that there is already adequate representation of international perspectives and impacts being provided by the State Department and Commerce, and that there are other avenues outside the VEP that are also used for coordination and alignment of cyber domain related activities:

- "State and Commerce already represent that. Given the fallout from Snowden, these are already really well considered. They have alternate intel sources."
- "Given that two of our closest allies also have public VEPs that very closely resemble that of the US kind of proves that we are already very closely coordinating cyber related equities, intel, and issues with members of the international community that matter to us, so why make the process more difficult by actually having someone sit at the table?"
- "We have very smart people working on this, they know the geopolitics, they know what's going on, they are aligning with our allies daily. Don't make the process more cumbersome."

It is worth noting that there were a handful of interviewees who had directly participated in ERB discussions and did not feel that the State Department was well positioned to represent international equities:

- "I don't think State has it covered. State has been hopelessly out of range and unprepared to address this topic in other venues with our coalition partners and allies. They have appeared absent and uninterested in helping the international community."

A Global Set of Equities Would Support the Development of Norms Around Vulnerability Exploitation

While a "world VEP" does not seem plausible due to the large number of diverse equities held by each country, the interviews highlighted the potential value a global set of equities could bring – particularly in supporting the development of global norms around the exploitation of vulnerabilities. Although not perfect, the US' VEP could serve as a starting point for the development of a general set of high-level equities that should be considered when a country is faced with the option of retaining or disclosing a zero-day vulnerability; the goal would not be to align operations or processes across countries, but outcomes:

- "It could be a good move for the US to say this is what we think the norms should be around exploitation and dissemination, and it should be part of international law. A unilateral declaration could really help move cyber norms in the right direction – which would ultimately be in the US' interest."

By actively (rather than passively) engaging others on a multinational level, the US establishes a public benchmark for our allies and partners, while also making ourselves an available resource (perhaps through a structured collaboration or education program) to both high- and low-capacity partners to support the development of their respective vulnerability exploitation (and broader cyber) policies and processes:

- "Our VEP isn't perfect, but it's a good benchmark for all other countries, particularly for our allies. We need to continue working with other nations who want to further their own cyber policies."
- "A lot of our high- and low-capacity partners have questions and are making decisions, and they're asking us for guidance and answers. If we can align their interests and outcomes with ours, we should be doing everything we can to actively support them."
- "I think other countries should have a similar process and should report on the general decisions that have been made. There is a divide between the military, law enforcement, and civilian populations in other countries that is much bigger than exists here, so parts of their governments often times do not know what others are doing or may not know that a process exists to do what they are talking about, and I think that's one area where the US could really support our partners. The US has a very strong and interconnected intel process."

The VEP Charter Also Serves as an Ethics Guiding Document

Nearly a quarter of interviewees (~21%) believed that the VEP charter is not merely in place for practical reasons, but also serves as a document to guide ethical decision-making around the retention or disclosure of newly discovered software vulnerabilities:

- "Fundamentally, the VEP is really about moral issues, not practical issues. It's about, 'Hey, we've got this new vulnerability, and how are we going to feel if we use it and don't disclose it and then some adversary uses it to take out a hospital and children die? Or a cybercriminal uses it to drain bank accounts and a million citizens lose their savings?'"

- "[The VEP] is about ethics. It's not about having some impact on the outcome of cyber security. It's not about the US Government disclosing vulnerabilities to make a more secure internet and software ecosystem, and it's usually misunderstood as being that."
- "Government is supposed to do more good than harm, and the goal is for the Government to make decisions that do the least amount of harm. There are always competing equities, and there will be times the Government needs to exploit a vulnerability for national security or significant LE efforts, but the VEP forces them to look at the other types of harm that they might cause. It forces them to go through that thought process. Good public policy should be rooted in good ethical theory. If we find a vulnerability in a widely used pacemaker, are we going to take that risk? I would hope not."
- "I don't think there's anything wrong with the VEP having a moral dimension to it in order to limit damage to the US and civilian population – which is its main intent."

Chapter Conclusion

My interviews with 19 VEP SMEs produced a robust set of findings centered around twelve emergent themes, several of which appear to independently confirm a number of the concerns highlighted by the public in Chapter 1. Similar to the views expressed by media and digital advocacy groups, the majority of VEP SMEs also believe that agency affiliation and majority IC representation on the ERB influences adjudication outcomes, and that an enforcement mechanism for the VEP is in fact needed; per the VEP SMEs, the fact that the annual VEP reports have not materialized is evidence enough that the process will not be consistently adhered to in its current state. Also in line with views expressed by the public in Chapter 1, several of the themes that emerged suggest that the current VEP places greater emphasis on government-oriented equities than public or social good-oriented equities; this includes the themes related to agency affiliation and majority IC representation, but is perhaps most noticeable in the belief expressed by VEP SMEs that the VEP really does need to do a better job in ensuring consumer and industry equities are sufficiently considered. Of course, other themes also emerged, such as industry's role in the vulnerability of their customers, and how the VEP charter could be used as a strategic tool to cultivate international norms around the exploitation of software vulnerabilities.

Although these findings provide me with a number of different directions to continue developing my research, this dissertation must remain appropriately scoped. As such, I will be pursuing the reoccurring theme of the VEP's deficient consideration of public or social good-oriented equities. While the publicly available literature initially suggested this theme, and my VEP SME interviews also indicated the existence of the same theme, I would like to assess the VEP using another method – specifically the application of an ethics-based framework to the VEP – to see if this theme of a deficiency in the consideration of public or social good-oriented equities also emerges. Ethics-based frameworks have been used across a wide range of

disciplines to better understand the link between macro-level structures (such as the VEP) and public or social good. I will expand on the use of these frameworks and my methodology in Chapter 3.

Chapter 3: Ethics Considerations

As highlighted in the conclusions of both Chapter 1 and 2, there is a common theme of public equities not being considered as robustly as they arguably should be by the Vulnerabilities Equities Process (VEP). In Chapter 1 we saw this demonstrated as an incongruence within the design of the charter itself; although the first paragraph of the charter clearly states that "the primary focus of this policy is to prioritize the public's interest in cybersecurity,"[294] that prioritization or concern for the consideration of the public's equities is not reflected in the charter's considerations. This sentiment is supported by the findings from Chapter 2, with interviewees specifically pointing out that the VEP – both in design and practice – places greater emphasis on government-oriented equities than those of consumer and industry stakeholders.[295] When taken into consideration together, these findings suggest that while the VEP charter may adequately consider the government-oriented equities of a zero-day software vulnerability disclosure, there is a deficiency in the VEP's consideration of public or social good oriented equities. One method used to investigate how well public policies take various stakeholders' equities into consideration is through its application to an ethics framework.

Ethics refer to broad moral principles, most often applied to questions regarding what "correct" behavior is (such as "right" versus "wrong") within a specific context (including in both a "scenario" and "cultural" sense, which is discussed further on in this section).[296] There is still no universally accepted framework for including ethics into conversations and decisions centered within the cyber domain – of which the VEP would fall under. The two main reasons for this are that (1) although we have seen progress in the past ten years, it remains – in general – an under-researched area of knowledge, and (2) there are many subdomains within "cyber" whose ethics considerations could be considered "context sensitive." While this section's objective is not to bridge that gap completely, it does aim to highlight the importance of including an ethics component to cyber-related public policy decisions, and suggests a new virtue-based framework to apply to public policy decisions specifically centered on software vulnerabilities. Finally, this chapter concludes with applying this new virtue-based framework to the VEP.

[294] White House, 2017b, p.1.

[295] Please refer to section "Consumer & Industry Equities Should Be Better Represented, But 'How' Is Unclear" of Chapter 2 for a comprehensive discussion of this finding.

[296] Ethics, 2022.

Previous Applications of Ethics in Cyber-Related Public Policy

We begin this discussion on the premise that every voluntary and participatory social construct – both informal (e.g., a group of friends) and formal (e.g., a democracy) – is founded on a set of core ethics values shared by those involved; an unspoken social contract by which all members agree to abide by in order to freely operate and exist within the boundaries of said social construct. These core ethics values are highly influenced by broader cultural contexts[297] (both individual and societal, which, themselves, do not always intermingle nicely), and therefore may not always be perceived as "right" by individuals from varying cultural backgrounds. And while this cultural dimension is important, it is also a deeply complex topic that genuinely requires a study primarily focused on those dimensions. As such, I will proceed with the acknowledgment that culture does play a formative role in which sets of ethics are core to specific groups, but will not expand further.

For macro-level entities such as governments, all public policies produced to govern and regulate should be firmly rooted in and reflective of their respective set of ethics values; if not, the potential imbalance between the populace's believed and perceived set of values may lead to unintended consequences.[298] Again, this only applies to governance structures which are voluntary and participatory in nature, meaning that the populace must be allowed to participate in actions that can transform the government's structure into one that they see more reflective of their values (as long as those actions do not violate the populace's core set of values [e.g., the deliberate and unlawful killing of one person by another]), and/or (2) the populace must be allowed to physically and freely exit from that governance structure ("physically" meaning that they can freely relocate to another geographic area outside of their current government's purview; this does not include individual succession from a country while also remaining within the geographic boundaries of that country, such as with the Sovereign Citizen movement in the United States). Since this research is focused on the cyber domain, I assert that the previous statement – by extension – also holds true for the cyber domain: all public policies produced by a government to govern and regulate aspects of the cyber (or "digital") domain should be firmly rooted in and reflective of their respective set of ethics values. This is not to say that ethics is the only factor considered by policy makers – others such as efficient allocation of resources, justice, and fairness are all priorities that must be balanced – but I do assert that all factors considered are abstracted means of operationalizing the underlying core set of ethics values that governance structures are built upon.

Although still fairly under-researched when compared to other subdomains of ethics, the ethics frameworks being developed and applied to public policy specifically with respect to the

---

[297] İbrahimoğlu et al., 2014.

[298] The potential form of these unintended consequences are highly dependent on the situation and context, and therefore will not be analyzed in this study.

cyber domain are increasing in number and variety.[299] As a sample of the variety, these areas of research now include "data and information (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including AI, artificial agents, machine learning and robots), corresponding practices and infrastructures (including responsible innovation, programming, hacking, professional codes and standards),"[300] and the design of digital technologies (including end-user privacy and monitoring).[301, 302, 303, 304, 305, 306] A key reason behind this increase in research is the proliferation of technology across nearly all facets of life, including industrial IoT, smart homes & cities, health care, finance, and law enforcement.[307] These approaches generally attempt to "embed" ethics as close to the design phase as possible, often allowing for feedback loops which act as "correcting" mechanisms to re-align the actual output or outcome with the pre-established ethical intent. Other approaches take a cost-benefit approach, attempting to account for all possible variables, assigning each a relative weight, and allowing the ensuing mathematics to define what constitutes a "good" or "bad" outcome – although this approach is far less common.[308] Through my review of this literature, I identified a notable gap: there does not appear to be any current ethics-based frameworks designed specifically for application to software vulnerability-centric public policy.

This variety in approaches highlights three general challenges encountered when attempting to apply ethics to the cyber domain:

1. It is a difficult task to take abstract ethics theories and apply them to concrete cyber domain scenarios. This is often further complicated by potentially conflicting ethical baselines of different actors and the context within which the scenario is taking place (e.g., it is possible for an action to be ethical in one context, and unethical given another context).
2. Inversely, it is equally as difficult to identify which ethics values or principles are present – let alone, "most important" – when addressing a cyber domain scenario. Again, this perspective is further complicated by all the intricate technical processes at play, the actors involved, and the surrounding context.

---

[299] Formosa et al., 2021.

[300] Floridi et al., 2018.

[301] Calvo & Peters, 2013.

[302] Dorrestijn & Verbeek, 2013.

[303] Ijsselsteijn et al., 2006.

[304] Roeser, 2012.

[305] Sinche et al., 2017.

[306] Garcia-Ceja et al., 2016.

[307] Markendahl et al., 2017.

[308] Smith, 2017.

3. The general lack of agreement on any level (e.g., approach type, ethics theory, appropriate values, etc.) across the various approaches presented throughout the literature demonstrates the fact that there still is no normative understanding of applied ethics to the cyber domain. The field is still very much in an exploratory phase of development.

A common example used to illustrate these challenges is through the examination of ethics in the context of a cyber conflict. In a traditional conflict between nation states, international law has established criteria that must be met in order for that conflict – or war – to be deemed ethically just. These include the open declaration of war by an appropriate governing authority, a justifiable reason for declaring war, and the use of force as a last resort.[309] While perhaps more clear-cut in the physical domains of war – sea, land, air, and space – the cyber domain blurs these lines of justification. The difficulty in attributing cyber actions to any specific nation state can make it challenging to answer the questions of "are we at war?" and "who are we at war with?"; is a military site or civilian being impacted by the actions of a state actor or non-state actor? – and are those actions intentional, or just an unintended consequence of potentially unknown interdependencies in a network? To further complicate matters, still-debated norms[310] on what constitutes an acceptable response to a given cyber action obscures the answer to "is the magnitude of my response in line with the magnitude of the cyber attack?" Studies such as the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* have attempted to clarify, deconflict, and establish norms related to actions in the cyber domain, but even they are challenged by the obscurity of cyber space – often relying on the term "jurisdiction"[311] which has no clear-cut application in the cyber domain; where does one country's boundaries or territory end and another's begin cyber space?

Even when discussed in the context of a nation's own assets or citizenry, this conversation of justified and ethical cyber action does not become any clearer. A common example referred to in this context is law enforcement's use of "alternative means" to catch criminals. Whether it be through the exploitation of a software vulnerability[312] or the hiring of a third-party to extract the desired information (colloquially known as "Access-as-a-Service"[313]), questions around the potential violation of privacy and civil liberties are raised; how do we determine when it is "right" to use these methods, what criteria is used to determine the individuals who these techniques are used on, and who makes the final decision? What distinguishes these third-party service providers from formal criminals, and how do law enforcement entities justify their

---

[309] Johnson, n.d.

[310] Katagiri, 2021.

[311] Patrick, 2019.

[312] O'Neil, 2001.

[313] For a more comprehensive read on this topic, I recommend Nicole Perlroth's book "This Is How They Tell Me The World Ends" (2021).

purchasing of these services when similar actions taken by a regular person could be deemed "criminal"? While the American public would certainly welcome additional cyber protections from the state and federal governments, most would not prefer it in the form of law enforcement entities having unfettered access to their digital lives; the marginal increase in security would not be worth the egregious loss of privacy. Where do we draw the line between justifiable "hunting" of cybercriminals and the violation of civil liberties?

The Importance of Ethics in an Increasingly Digital Society

As previously noted, the application of ethics to the cyber domain – albeit increasing – remains a relatively small body of knowledge. And this is not because researchers do not see value in further developing this area, but because it can be challenging to apply ethics to the context sensitive and fluid cyber domain. However difficult, though, it is becoming increasingly urgent that research in this area be given more attention. The speed with which technology is advancing, coupled with the ever-increasing rates of adoption due to the commercialization of these technologies, has changed how humans live on a fundamental level. The relationships we have with ourselves, our environment, and one another have forever changed; we are more connected than ever before (on both macro and micro levels), have access to more information than ever before, and are – in a very literal sense – reliant or dependent on these systems and data at both the individual and group/social level.[314] In many ways, all these relationships are being "mediated" by those enabling technologies in forms that are effectively outside of our (the consumer's) control – all of which raise valid ethical questions around who is responsible for putting those mediating powers in place, and the impact that these digital technologies are having on our well-being (again, at both the individual and group/social level).[315, 316]

Ethics are important at the societal level because they shape the type of world we live in; what is socially deemed moral, right, or necessary directly influences public opinion (i.e., what is viewed as socially acceptable and preferred), which in turn – at least in democracies – informs the legal parameters installed that shape all facets of life (e.g., personal, commercial, political).[317] As Floridi (et al., 2018) explains, this concept of ethics-informed societal structures translates into the digital realm as three interconnected and interplaying components: digital ethics (the moral evaluation of issues related to the digital realm), digital governance (the establishing and implementation of policies, procedures, and standards to guide the proper development and use of the digital realm), and digital regulation (the mechanisms available to enforce compliance upon relevant agents in accordance with the system of rules put in place via the digital

[314] Floridi, 2014b.

[315] Formosa et al., 2021.

[316] Vallor, 2018.

[317] Floridi et al., 2018.

governance component).[318] Floridi asserts that while the foundational digital ethics assumed by a social structure influences the shaping of the digital governance and digital regulation practices that follow, the outcomes or results of those digital governance and digital regulation components can also influence changes within the data ethics foundation. For example, even though the value of digital privacy within a given society may be very high, members of this social structure may be willing to change that value to give up an incremental amount of data privacy if they see that doing so allows the digital governance and digital regulation components to efficiently and effectively dismantle child exploitation rings.

It is worth noting that the digital governance and digital regulation components themselves (and the resulting outputs) are neither moral nor immoral; it is only after their outputs are viewed within the context of their respective digital ethics foundation that they take on these "morality" qualities. Floridi (2018) asserts that this moral evaluation of governance and regulation practices is necessary because while the regulation component might tell us what is legal and illegal, and the governance component might tell us how to get to an end point through a given system, neither is sufficient to help us determine what is *best* to develop a better society; that requires a moral evaluation, and that moral evaluation must be rooted in some set of ethics (hence, the necessity for digital ethics). This helps us better understand why an ethics framework is important, in particular when it comes to new and pervasive technologies to ensure that their development and application are in alignment with what is needed to develop a "better" society. Taking this one step further, we can use these ethics frameworks to not only evaluate the desirability of current states (prompting change if the outputs do not align with our ethics foundation), but also to evaluate the desirability of potential future states and influence them accordingly if feasible alternatives exist that better promote social well-being.[319, 320, 321]

Again, by applying the before mentioned concepts in a digital context, we can better understand its importance: if our ethics foundation is rooted in a societal desire for all digital technologies (in both their design and application) to improve "digital well-being" (meaning that they support humans in living a "good" life), then the digital governance and digital regulation components should both guide and incentivize agents (e.g., tech developers, platform providers, resellers, etc.) to evaluate the consequences associated with their technology in such as way where beneficial consequences are promoted (e.g., promote institutional participation in platforms that offer high-quality educational courses for no cost) and potentially harmful

[318] Floridi et al., 2018.

[319] Feng et al., 2018.

[320] Garcia-Ceja et al., 2016.

[321] Kocielnik, et al., 2013.

consequences are avoided (e.g., disable social media "doom scrolling" features for users under the age of 18).[322, 323]

Circling back to how this section began, we must begin designing ethics frameworks to address the novel challenges that we as a society will repeatedly face as the digital realm continues to advance. And it is precisely because of this alarming rate of technology innovation that these frameworks must be flexible; if they are designed too rigidly, they will quickly become obsolete. And it is because of this unbridled speed of commercial innovation that public policy entities play a vital role in ensuring that a level of reflective equilibrium exists to protect the well-being of the people (in alignment with the appropriate ethics principles) from potentially detrimental technology advancements (which are generally driven by monetary goals).[324, 325] Just because a capability "could" exist does not mean it necessarily "should" exist (tying back to the idea of promoting beneficial consequences and avoiding harmful ones), and this begins drawing us into the realm of public policy. Framing this in the context of the VEP, does the fact that the Federal Government has the capacity to identify and exploit new software vulnerabilities mean they should be allowed to do so without restriction? Should they be required to make a good-faith effort to consider the potential impacts the exploitation of a software vulnerability might have on entities outside of the government, such as consumers and industry stakeholders? These ethics considerations and their interplay with governance and regulation help shape the society we live in and the well-being of society as a whole.

Social Good

Since a key portion of this discussion involves the idea of social well-being – or "social good" – it is worth taking a moment to clarify what I mean by the term. The term "social good" is often used interchangeably across the ethics literature with other terms, particularly those of "public good" and "common good" – even though there are nuanced yet important distinctions between them.[326, 327] *Social good* is understood to be "an action, service, or product that is of benefit to the functioning or well-being of society, or that otherwise advances the interests of humankind,"[328] which occurs "at the intersection of 'social good domains,' 'unconventional systems of change,' and 'innovative technologies and approaches,'"[329] and this is the definition

---

[322] Roeser, 2012.

[323] Burr et al., 2020.

[324] Mittelstadt, 2017.

[325] Vallor, 2016.

[326] Verdugo, 2013.

[327] Hooker, 2009.

[328] Garlington et al., 2020, p. 196.

[329] Mor Barak, 2018, p. 8.

that this research study will use going forward. This definition, however, differs from (1) *public good* in that public good is viewed as resulting from public funds or public policy, whereas social good is generally viewed as resulting from the collaboration of partners that would not normally collaborate (i.e., their collaboration is not dependent on the existence of public funds or public policy);[330, 331] and differs from (2) *common good* in that social good "is not tied to a specific community's goals, norms, or resources,"[332] and is thought of on a more macro level (e.g., national or global level). When looked at as a whole, we can see that the concept of social good is much more expansive in its perspective on systems, means, and collaborators of change and well-being.

The related topics of power structures and solidarity are important concepts to consider when discussing social good. Historically, the power structures present within a society have influenced the materialization of what "good" or "beneficial" actions for a society look like; in these instances, those in a decision-making position may say "society," but are actually referring to the subset of their society with power or financial wealth.[333] It is easy to see how this skewing becomes problematic when trying to address true social good concerns, so being cognizant and acknowledging of their existence is important.

The cultivation of solidarity, however, is one way to overcome these power differentials that exist to promote activities or actions that push the society as a whole in the direction of social good. *Solidarity* in the literature is defined as "a concern for the well-being of the other with the universality of human rights and the protection of dignity"[334] through the development of a relationship that "is not one of equals in power [or] role,"[335] but in the establishment of equality of persons. It calls for the privileged to act in the interest of the vulnerable – "those whose dignity is threatened"[336] – and to hold themselves accountable in acting because they have the means to do so (whereas the vulnerable and disadvantaged do not). Accountability plays a key role in developing solidarity, because it is through accountability that social trust can be cultivated within communities (and on a macro-level within societies). This importance of accountability towards one another on a human level and its impact on the vulnerable is eloquently captured by Clark (2014):

> "If your pain cannot change me and my pain cannot change you, then the relationship cannot be one of solidarity, even if basic needs are being met. […] It is not enough to recognize and fight injustice; vulnerability and participation

[330] Mor Barak, 2018.

[331] Garlington et al., 2020.

[332] Mor Barak, 2018, p. 2.

[333] Garlington et al., 2020.

[334] Ter Meulen, 2016, p. 525.

[335] Clark, 2014, p.129.

[336] Garlington et al., 2020, p. 199.

> grounded in the one human family must also be present. I must see your dignity bound up with mine."[337]

It is through this concept of social good – particularly when viewed in relation to the complementary concepts of power structures, solidarity, and accountability – that we begin to understand the intimate connection between social good and public policy. Social good is an intangible symbol of the relationships and outcomes that are valued by the citizenry of that society; and through the democratic empowerment of those public entities representing the citizenry, public policy acts as the facilitator in making those relationships and outcomes come to fruition. As Shukla (2017) asserts, "without a wholesome, systematic, and effective concept of social good, our public policy – no matter how vigorously implemented – will hardly succeed in accomplishing its task."[338]

Looking at the VEP through the lens of public policy, we can use the related concepts of power structures, solidarity, and accountability to examine how well the VEP considers social good. The VEP – even in its previously classified form – most definitely sits at the crossroads of innovative technologies (referring to the advent of the cyber domain) and unconventional systems of change (referring to how the cyber domain has fundamentally changed the way humans experience life) – which were noted above as two key identifiers of entities that can drive social good. The presence of a power structure is evident, with the VEP holding a unique position. Established at the highest level of our federal system (the Executive Office of the President), the decisions coming out of the VEP have the potential to impact a vast number of people – both within the US, as well as externally. And given that the VEP is composed primarily of intelligence and law enforcement related entities, it is not difficult to see how their final decisions could potentially be skewed towards government-oriented equities if their scope of equities considerations is not deliberately designed to broaden that scope. In the context of this power structure, the Equities Review Board (ERB) (the decision-making entity of the VEP) would be considered the "privileged" because they retain all the decision-making power, and the citizenry would be considered the "vulnerable" because they effectively have no say in the process or outcomes yet are impacted by the decisions. Given this power differential, the concept of solidarity can be used to examine how well the privileged act in the interest of the vulnerable. Since there is virtually no publicly available information about the VEP aside from the charter itself, I cannot make a robust determination on this; however, it is evident (as highlighted in Chapters 1 and 2) that the charter is deficient in its consideration of public oriented equities, which would suggest that the ERB is not taking in all the information necessary to know if they are truly acting in the best interest of the vulnerable. The absence of accountability in the VEP – identified by the lack of an enforcement or oversight mechanism – undermines the Federal

---

[337] Clark, 2014, p. 129.

[338] Shukla, 2017, p. 20.

Government's ability to cultivate public confidence in the process; this is arguably particularly important for a policy such as the VEP because all the associated discussions, decisions, and outcomes unfold outside of the public's view, so there are no other mechanisms available to promote public confidence. When considered together, the absence of accountability and inability to demonstrate solidarity in the presence of such an unequal power structure (being that the VEP is a federal level policy with far-reaching impacts) suggests that the current design of the VEP charter does not robustly account for social good.

Given that the VEP is a federal level policy whose outcomes directly impact the public, I suggest using an ethics-based virtue framework in the next section as a viable means for addressing the VEP's deficient consideration of social good.

A Virtue Framework for Software Vulnerability-Oriented Public Policy Processes

As mentioned earlier in the "Previous Applications of Ethics in Cyber-Related Public Policy" section of this chapter, a review of ethics-based frameworks currently developed for the cyber domain revealed a notable absence of an ethics-based framework specifically designed for application to software vulnerability-centric public policy. This is significant because Chapter 1 and 2 highlighted the VEP's deficiency in considering public or social good-oriented equities, so a need for such as framework exists. To address this absence, I have developed an ethics-based framework designed for application to software vulnerability-centric public policy, and used this method to determine how satisfactorily the VEP adheres to ethics considerations that are important to software vulnerability-oriented public policy and the promotion of social good. It should be noted that since I developed this ethics-based framework during the course of this study and it has been peer-reviewed for the purpose of this dissertation, this is the first time this new ethics-based framework has been applied.

Before I began development of my virtue-based ethics framework, I reviewed the ethics literature for the various types of ethics frameworks most commonly applied to the cyber domain. From this review, I found that the utilitarian and consequentialist frameworks were the most commonly applied to the cyber domain. Utilitarianism seeks to maximize "happiness" for the most people possible.[339] One issue encountered with this framework, however, is how to operationalize "happiness" – particularly in the context of software vulnerabilities. Is it simply protected or unprotected, patched or unpatched? Are we willing to sacrifice some security so that our personal devices such as cellphones can connect to all of our other devices seamlessly and automatically? The answer to these questions most likely varies from person to person, and perhaps even on the particular scenario. Based on these complexities – and given the fact that my goal was to develop a light-weight framework that can be easily overlayed upon current policies

[339] Driver, 2014.

and process – I determined it was not practical to move forward with a utilitarian-based framework. Consequentialism, on the other hand, judges how ethical a decision is based on the consequences it causes.[340] This framework, however, is often critiqued on the difficulty around understanding the complete set of outcomes that a singular decision can cause,[341, 342, 343] and when we place this in the context of software vulnerabilities it becomes even more complex; it is virtually impossible to know prior to a decision exactly who else is aware of and has access to a vulnerability, who has the skills and motive to exploit it, all of which is compounded by the difficulty in establishing attribution afterwards. Again, because of these complexities, it was not feasible for me to continue forward with a consequentialist-based framework. Aside from utilitarianism and consequentialism, though, there are other ethics frameworks – albeit less often applied to the cyber domain – and from these other frameworks I decided to proceed with "virtue theory" (specific benefits of leveraging this framework will be discussed later in this chapter).

Virtue Theory

Virtue theory is an ethics approach rooted in the idea that "virtues" are global traits that endure across situations and manifest themselves in a wide range of mental states and behaviors.[344] It has become established and acknowledged in the field of philosophy as a legitimate alternative to other ethics-based theories, and has been leveraged across a wide range of disciplines to better understand the link between social good and macro-level structures, including political science,[345] policy analysis,[346, 347, 348] organizational studies,[349, 350] public administration,[351] management,[352] and social work.[353, 354, 355]

---

[340] Sinnott-Armstrong, 2019.

[341] Sinnott-Armstrong, 2019.

[342] McElwee, 2009.

[343] Mukerji, 2013.

[344] Wright et al., 2021.

[345] Bartlett, 2002.

[346] Lejano, 2006.

[347] Szostak, 2002.

[348] Szostak, 2005.

[349] Dutton et al., 2006.

[350] Weaver, 2006.

[351] Overeem & Tholen, 2011.

[352] Wright & Goodestein, 2007.

[353] Adams, 2009.

[354] Banks & Gallagher, 2009.

[355] McBeath, 2016.

Virtue is defined as "the application of ethics or morals in a practiced, habitual manner, beyond single expressions of moral or good behavior. […] Virtuous action is contextual and based on collective knowledge and understanding."[356] Virtues differ from habits in that habits are mindless behaviors, whereas virtues are rooted in "reasons;" they are conscious decisions made by a rational person (or entity) to act in a specific way rather than in another.[357] Take the virtue of justice as an example. Making a decision or performing an action that happens to also be just does not make you a just person; you must have the intent to perform just actions and then follow through with that intent in order for "justice" to be one of your virtues. To determine whether an individual is capable of making virtuous decisions, Aristotle established four pre-requisites that must be met:[358]

1. Rational reasoning is required, meaning reasoning free from raw emotions or passions;
2. The individual must have the capacity to understand daily life situations;
3. The individual must have the will to act in "good" ways, while also having the will to avoid ways that are harmful (both to themselves as well as to others); and,
4. The individual must be a free moral agent, meaning one "who rationally deliberates on the goods that he desires, the actions that he wants to perform, and the virtues that he wants to practice."[359]

From this definition we can better understand how an individual's, entity's, or society's core set of virtues guide their decision-making and behavioral patterns. Inversely, one can analyze the decision-making and behavioral patterns of an individual, entity, or society to better understand their underlying core set of virtues. In the case of the VEP, we could use the annual adjudication reports – if they contained the appropriate type and amount of information needed – to identify decision-making patterns to gain a better understanding for what core virtues might be present. With the reports not being published, however, this straightforward approach is not possible.

Developing the Virtue Framework

Virtue theory provides the best ethics-based foundation to develop my own framework for application to public-oriented software vulnerability processes for several reasons. First, virtue theory is an established and accepted approach that has been used across a range of public-oriented disciplines to better understand the link between social good and macro-level structures; this includes their use for examining the relationship social good and power structures, which provides me with a strong foundation build off. Second, the use of virtues allows the framework

[356] Garlington et al., 2020, p. 198.

[357] Annas, 2007.

[358] Aristotle, n.d.

[359] Shukla, 2017, p. 27.

to operate at a less abstract level without being overly specific; this will maximize the flexibility and applicability of the framework. Third, unlike with other ethics-based frameworks like utilitarianism (perhaps the most commonly used ethics-based framework in public policy, seeking to maximize "happiness"), virtue theory allows us to develop a framework that moves beyond aspects that may be related to specific religious beliefs or practices, and focus rather on components that reflect desired professional public stewardship. This is particularly important for public policy application in the United States (or like countries) where the separation of church and state exists. And finally, the use of a virtue-based framework allows us to identify underlying virtues that remain relevant over time, rather than other agents or dimensions which could evolve as time and context both evolve; by taking this approach, my virtue-based framework can support decision-makers as they consider tradeoffs that may impact long-term public value. This enables the resulting framework to be flexible and capable of adapting to new technologies, agent-sets, and contexts as they arise. Given the speed of technology innovation, this is particularly important; a rigid agent-based framework will have limited utility and quickly become obsolete.

As suggested in the four points above, the purpose of this framework is not to overly burden public policy processes or entities with ethics considerations (context is still very important to the determination of what is moral, right, and necessary – especially when dealing with processes that touch on national security), but to ensure that these public policies are in fact adequately considering ethics and, by extension, social good. I propose the following virtue-based framework as a lightweight framework that can be overlayed on top of existing processes to further promote reflective equilibrium – supporting decision-makers in taking the entire context of a scenario into account (including all relevant stakeholders), and actively identifying and correcting any bias present when making a software vulnerabilities focused policy decision. This allows for the most informed decisions possible, supporting decision-makers in their balancing of potential consequences with the context and feasible options available. Through this support, my virtue framework facilitates decision-makers in ensuring their processes and resulting decisions are maximizing social good to the furthest extent possible.

The framework is composed of a "virtuous decision-making qualification" section (used to qualify the public policy decision-making entity's capacity to make virtue-based decisions), and four stand-alone virtues (non-maleficence, beneficence, solidarity, and situational fairness) that assess a different aspect of a public policy entity's decision-making behaviors. Below I expand on why I selected these four virtues and what each entails.

Virtuous Decision-Making Qualification

The first part of this virtue framework is used to qualify a public policy process or decision-making entity's (and all sub-entities that may compose said entity, such as a panel or board)

capacity for making virtue-based decisions. This qualification is composed of three questions (which have been adapted from Aristotle's requirements for virtuous decision-making):[360]

1. Is the process or entity "rational" in its reasoning? (meaning that its reasoning is free from raw emotions or passions);
2. Does the process or entity have the capacity to understand daily life situations? (meaning it must have the ability to understand how the resulting decision will impact the daily lives of the public and other relevant stakeholders);
3. Does the process or entity have the will to act in ways that optimize social good? (meaning that during the decision-making process, it must [in good faith] strive to make decisions that promote socially beneficial consequences while minimizing potentially harmful consequences).

A process or entity can either "satisfy," "partially satisfy," or "not satisfy" the three qualifying questions above. The lowest "satisfying" rank assigned to any of the three questions is used to determine the process or entity's overall virtuous decision-making qualification. For example, if an entity obtained two "satisfy" qualifications and one "partially satisfy" qualification to the three questions above, the entity would be deemed partially capable of making virtue-based decisions. Similarly, if an entity obtained two "satisfy" qualifications and one "not satisfy" qualification to the three questions above, the entity would be deemed not capable of making virtue-based decisions.

If a process or entity satisfies all three qualifying questions, the remainder of the framework can be reliably applied, and the results used to guide improvements to increase the process' social good output. If a process or entity does not fully satisfy all three qualifying questions (meaning they have at least one "partially satisfy" or "not satisfy" qualification), then the remainder of the framework can be applied only in research capacity to identify other areas for improvement – although achieving a "satisfy" qualification on all three qualifying questions should be prioritized; other efforts can be deemed moot until this occurs.

Identification of Virtues

Through my review of other cyber domain related virtue frameworks (see Table 2), I found that a wide variety of virtue sets have been used; some of the most common tend to be beneficence (the promotion of human well-being), contextual or situational fairness (the consideration of all elements that surround a scenario to avoid bias), justice (the promotion of fairness and equality), and accountability (the obligation to account for one's actions). Given the extensive set of virtues, I will not review each one to explain why I chose not include specific virtues in my virtue framework. Instead – and in the sections below – I will explain why the four virtues of non-maleficence, beneficence, solidarity, and situational fairness are most appropriate

[360] Aristotle, n.d.

and applicable for use in my virtue framework designed for application to public-oriented software vulnerability processes.

Table 2: Summary of Virtues Identified in Ethics-Based Frameworks for the Cyber Domain

Source	Virtue Sets
The Menlo Report (2012)	1) Respect for Persons, 2) Beneficence, and 3) Justice
British Academy & Royal Society (2017)	1) Independence, 2) Deep Connection to Diverse Communities, 3) Cross-Discipline Subject Matter Expertise, 4) Closeness to Decision-Making Processes, 5) Durability & Transparency, and 6) Nationally-Focused but Globally-Relevant
Floridi et al. (2020)	1) Falsifiability & Incremental Deployment, 2) Safeguards Against Manipulation, 3) Contextualized Intervention, 4) Contextualized Explanation & Transparency, 5) Privacy Protection & Data Subject Consent, 6) Situational Fairness, and 7) Human-friendliness
Loi & Christen (2020)	1) Privacy, 2) Data Protection, 3) Non-Discrimination, 4) Due Process & Free Speech, and 5) Physical Integrity
Morgan & Gordijn (2020)	1) Privacy, 2) Protection of Data, 3) Trust, 4) Control, 5) Accountability, 6) Confidentiality, 7) Responsibility of Business to Use Ethical Codes of Conduct, 8) Data Integrity, 9) Consent, 10) Transparency, 11) Availability, 12) Accountability, 13) Autonomy, 14) Ownership, and 15) Usability
Van de Poel (2020)	1) Security, 2) Privacy, 3) Fairness, and 4) Accountability
Weber & Kleine (2020)	1) Efficiency & Quality of Service, 2) Privacy of Information & Confidentiality of Communications, 3) Usability of Services, and 4) Safety
Formosa et al. (2021)	1) Beneficence, 2) Non-maleficence, 3) Autonomy, 4) Justice, and 5) Explicability

Before proceeding, please note that all the following virtues should be considered at the national level for two key reasons. First, given how regulatory complexities and sensitivities around software vulnerabilities vary between countries (even among allies and partners), considering each virtue at a global level would be overly burdensome and an exercise in futility. And second, even though we may not be able to feasibly consider these virtues at the global level, we should consider them at the national level given our national-level interconnectedness and dependencies in the digital domain.

Non-maleficence

The virtue of "non-maleficence" in the context of my virtue framework is the idea that the decisions being made by a public policy process or decision-making entity should not be made with the intention of causing harm to humans or to their social fabric. As the literature shows, "harm" enacted through the digital domain can manifest in many forms, such as reputational, psychological, or monetary harm resulting from a data breach,[361] physical harm resulting from a

[361] Formosa et al., 2021.

vulnerability exploitation (such as with Stuxnet[362] which caused physical damage to machinery),[363] and systemic harm resulting from the degradation of public trust when a publicly sponsored or hosted database or transaction is compromised.

It is worth noting that the topic of justifiable harm is consistently debated within the ethics literature – primarily along the lines of what constitutes "harm," and how do we measure the "severity" of harm across different forms and contexts.[364] And while there is no universally agreed upon answer, the general consensus seems to be yes, there are scenarios and contexts that can justify varying types and degrees of harm[365] – even within public policy. There are far too many "types" and "degrees" of harm discussed through the ethics literature as a whole than I can review in this section, but a common example referred to in the field of cybersecurity is whether the potential harm of "privacy violation" inflicted by surveillance is justified by law enforcement in their pursuit to catch cybercriminals.[366]

While I personally agree with the ethics literature in its assessment that the philosophical principle of justifiable harm exists within certain contexts, I am choosing to not carry that principle over into my virtue framework. My reason for this is that the virtue framework I have developed is designed to determine whether the behaviors or decisions of a specific entity tend to align with the four virtues I have outlined – while also remaining lightweight enough that the exercise of applying my virtue framework is not overly burdensome; if it is overly burdensome will not be employed at all. To achieve this for the virtue of non-maleficence (which can be particularly complex), I have chosen to abstract away from the infinite layers of potentially justifiable harm and condense it down to the belief that any level of *intended* harm violates this virtue.

Beneficence

The virtue of "beneficence" in the context of my virtue framework is the idea that the decisions being made by a public policy process or decision-making entity should have the ultimate objective of maximizing the benefit produced for humans and the broader social good. Like with the virtue of non-maleficence, "benefits" realized through the digital domain can manifest in many forms, such as improvements in public trust when cybersecurity best practices

---

[362] Uncovered in 2010, Stuxnet was a multi-part computer virus (categorized as a "worm") that was originally spread through infected USB sticks. The virus is most often associated with Iran's Natanz uranium enrichment facility, but did spread and impact networks in other countries (generally causing computers to repeatedly crash and reboot) and has since been modified to target other critical infrastructure. The Stuxnet virus was engineered by stringing together several previously-unknown software vulnerabilities ("zero-days), ultimately causing physical damage to the cyber-physical systems (primarily centrifuges). In the case of Natanz, Stuxnet ultimately reduced Iran's uranium enrichment capabilities by 30% during the time it went undetected (roughly 2008 – 2010).

[363] Hildebrandt, 2013.

[364] Formosa et al., 2021.

[365] Harcourt, 1999.

[366] Simone, 2009.

are implemented on public systems, and economic benefits resulting from the increased use of digital financial transactions when consumers and vendors have confidence in the systems they have available.[367]

This virtue, however, is unique in that it requires the decision-making entity to be aware of previously made decisions in order for them to effectively assess whether their next decision will have beneficial or harmful consequences. In some instances, a series of decisions when viewed independent of each other may each appear to produce benefits. However, the same set of decisions when viewed at the aggregate level – in their chronologically decided order and within the proper context of each other – can in fact inflict harm.[368] This is especially true when we think about software vulnerabilities. When thought of independent of each other, there does not seem to be too much cause for concern; however, when strung together to create exploits (e.g., Stuxnet[369]), we can see how much damage (physical, financial, reputation, psychological, etc.) they can cause.

Solidarity

The virtue of "solidarity" in the context of my virtue framework is the idea that the decisions being made by a public policy process or decision-making entity should be done so with concern for – and in the interest of – the vulnerable.

The absence of solidarity in ethics-based frameworks for the cyber domain is a key gap that currently exists in the literature. While several mention "trust" and "accountability" (and it can be argued that trust and accountability are components of solidarity), neither truly captures the essence of what solidarity embodies. This virtue of solidarity helps us transcend the power hierarchies that exist between the citizenry and the policy-/decision-makers, providing a link between the two based on the equality of persons rather than the role of power (for a refresher on

---

[367] Awojana & Chou, 2019.

[368] Floridi, 2013.

[369] Uncovered in 2010, Stuxnet was a multi-part computer virus (categorized as a "worm") that was originally spread through infected USB sticks. The virus is most often associated with Iran's Natanz uranium enrichment facility, but did spread and impact networks in other countries (generally causing computers to repeatedly crash and reboot) and has since been modified to target other critical infrastructure. The Stuxnet virus was engineered by stringing together several previously-unknown software vulnerabilities ("zero-days), ultimately causing physical damage to the cyber-physical systems (primarily centrifuges). The exploit was executed as follows: (1) Stuxnet enters a system running on Win OS via a USB stick and uses stolen digital certificate to evade automated-detection systems; (2) Stuxnet then spreads to additional systems running Win OS on the private network and searches for machines made by Siemens – specifically S7-300 PLCs with variable-frequency drives; (3) Once on a system, Stuxnet infects Siemens' "Step 7" SCADA control software via a key communications library; (4) Malware is then installed onto the DB890 memory block of the infected Siemens S7-300 PLC, which monitors the system; (5) When the malware detects a centrifuge motor spinning between 807 Hz and 1,210 Hz, the malware periodically modifies the motor's frequency to 1,410 Hz, then to 2 Hz, and then to 1,064 Hz, causing the centrifuge to spin itself to physical failure; (6) The malware then reports false feedback from the PLC to the control software by not disclosing the frequency modifications made to the centrifuge motor, making identification of the issue virtually undetectable. In the case of Natanz, Stuxnet ultimately reduced Iran's nuclear enrichment capabilities by 30%.

this topic, please revisit the "Social Good" section above). This is incredibly important for and relevant to public policy because we often have a policy making entity (the "privileged") making decisions on behalf of the citizenry (the "vulnerable"); the citizenry is considered the vulnerable in this context because they often do not have any direct influence over public policy related decisions where a group or process is making determinations on their behalf – and this is exponentially true for public policy decisions involving the cyber domain. As such, having a virtue such as solidarity included within a framework helps bridge that gap – not only by providing a humanity-rooted link between the citizenry and the decision-makers, but also by cultivating public trust through the implied commitment to (1) act with concern for the vulnerable, and (2) be held accountable for the decisions made.

Situational Fairness

The virtue of "situational fairness" in the context of my virtue framework is the idea that the decisions being made by a public policy process or decision-making entity should take the entire context of the decision into account and actively ensure that the final decision is not being unfairly biased.

Situational fairness is defined as "the idea that decisions may be amalgamated from factors that are not of obvious ethical importance, and yet collectively constitute unfairly biased decision-making."[370] The concept of situational fairness (also referred to as "contextualization") has only recently been included in cyber-related ethics frameworks – although almost exclusively in the context of artificial intelligence or machine learning.[371, 372] The inclusion of situational fairness in public policy (both generally, as well as specifically for cyber-related policy decisions) is necessary to ensure that no single or set of stakeholders or scenarios are given an unfair level of attention (or lack thereof) which may result in a biased policy decision. This works both in favor of the citizenry (by ensuring that they – both as a whole and as specific vulnerable groups – are provided adequate representation) and the policy-/decision-makers (by ensuring that their legitimate concerns related to broader social good are given adequate weight).

Discussion on These Virtues

Public policy development and decision-making is no easy feat. Attempting to balance several variables, stakeholders, stakeholder-specific needs, potential threats, and contexts is very difficult – and making decisions that have purely beneficial impacts is not always feasible; this is especially true for public policy development and decision-making in the context of national security. It is important that we acknowledge and remain sensitive to the reality of these potentially uncomfortable scenarios and their associated options.

---

[370] Pedreshi et al., 2008.

[371] Pedreshi et al., 2008.

[372] Floridi et al., 2020.

With that in mind, though, public policy developers and decision-makers are public servants acting on behalf of the citizenry, and therefore should be trying to balance all the variables before them in a way that maximizes the social benefits produced while minimizing the harms inflicted. My virtue framework outlined above aims to support public policy developers and decision-makers in considering their potential impact on social good when faced with software vulnerability decisions. I specifically selected the four virtues of non-maleficence, beneficence, solidarity, and situational fairness to support public policy developers and decision-makers in balancing the potential consequences with the context and feasible options presented to them in a rapidly evolving cyber domain.

Non-maleficence and *beneficence* aim to support public policy developers and decision-makers in understanding whether a decision they are about to make will likely produce more social benefits or social harm. Again, as stewards of the public, they should be striving to do more good than harm, but in certain contexts (like national security scenarios) causing zero harm is not always possible. It is for these instances in particular that my virtue framework aims to support public stewards in understanding the potential good produced by a decision in relation to the potential harm so they can make the most informed final determination from an ethics perspective.

In a similar fashion, *solidarity* and *situational fairness* aim to support public policy developers and decision-makers in understanding whether the decision they are about to make demonstrates solidarity given the scenario they are faced with. Again, what is deemed moral, right, or necessary is highly dependent on the context – and this is especially true for national security scenarios – so ensuring that the context of each scenario is being accurately represented in its entirety is very important. If a scenario is being unfairly, inaccurately, or otherwise represented in a biased manner, that will not only directly impact the final determination made, but potentially increases the likelihood of unintended consequences. Through the lens of solidarity and situational fairness, we can ask the question: Given the context of this specific scenario and the feasibility of all possible options, is the decision-maker (the "privileged") still acting with concern for and in the interest of the citizenry (the "vulnerable") who do not have a seat at the decision-making table? The answer to this question – when asked by an entity who meets the virtue framework prerequisites – aims to guide the decision-maker in making the most informed final determination from an ethics perspective.

Applying the Virtue Framework to the VEP

Now that I have operationalized each virtue and discussed how they fit within the framework, I will apply my virtue framework to the VEP to determine how well it aligns with each virtue, and will then use those findings to identify particular areas where additional steps should be taken to increase the VEP's robustness in its consideration of social good. As a reminder, I explained earlier in the "A Virtue Framework for Software Vulnerability-Oriented

Public Policy Processes" section that the overall objective for developing this virtue framework was to have an additional method to determine how satisfactorily the VEP adheres to ethics considerations that are important to software vulnerability-oriented public policy and the promotion of social good. As such, the determination reached in each of the four virtue sections will be aggregated to identify a conclusion as to the VEP's current ability to promote social good through its vulnerability adjudications. The VEP in particular is a good candidate for application of my virtue framework because (1) it is a federal-level public process that makes decisions related to the retention or dissemination of software vulnerabilities, and (2) being that the VEP operates purely at a classified level, all related information, deliberations, and final decisions are done completely outside of the public's view. This means that even though the decisions made within the VEP can have potentially widespread public ramifications, there exists a relational gap between the VEP and the public – and any time a gap of this nature exists, valid ethics questions around decision-making and decision-makers are raised.

Virtuous Decision-Making Qualification

Before I begin assessing the VEP against the four standalone virtues of non-maleficence, beneficence, solidarity, and situational fairness of my virtue-based framework, I must first qualify the VEP's decision-making component – the Equities Review Board (ERB) – for its capacity to make virtue-based decisions. To do this, I assign a "satisfied," "partially satisfied," or "not satisfied" determination to the following three questions:

1. **Is the ERB "rational" in its reasoning?** This prerequisite aims to determine whether the ERB's reasoning is free from raw emotions or passions. Given that the VEP charter requires the ERB's determinations to be rooted in the recommendations of subject matter experts, I determine this prerequisite is satisfied.
2. **Does the ERB have the capacity to understand daily life situations?** This prerequisite aims to determine whether the ERB has the ability to understand how their determinations will impact the daily lives of the public and the other stakeholders they represent. Given that the majority of ERB members are affiliated with either the intelligence or law enforcement communities, I believe the ERB does have the ability to understand how their determinations will impact the daily operations of those stakeholders. There are other stakeholder groups though – such as consumers and industry – that do not appear to be well represented within the ERB,[373] so it is questionable whether the ERB currently has the capacity to truly understand the impact their determinations will have on the daily lives of these stakeholder groups. For this reason, I determine the ERB only partially satisfies this prerequisite.
3. **Does the ERB have the will to act in ways that optimize social good?** This prerequisite aims to determine whether the ERB (in good faith) strives to make decisions that promote socially beneficial consequences while minimizing potentially harmful consequences.

[373] Please refer to the "Qualitative Research & Analysis" section of this research study.

> This prerequisite is slightly more difficult to address. The VEP charter does state that its primary focus "is to prioritize the public's interest in cybersecurity and to protect core [information systems] and the U.S. economy through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes."[374] However, given that (1) the ERB is primarily composed of members affiliated with either the intelligence or law enforcement communities, and (2) that we already established in the previous prerequisite that the ERB does not appear to well-represent other stakeholder groups that would need to be considered when addressing the topic of "social good" (e.g., consumers), it is questionable whether the ERB has all the information necessary to optimize social good during their determination discussions. For this reason, I determine the ERB only partially satisfies this prerequisite (the VEP charter reflects the *desire* to optimize social good, but it is unclear if the ERB *actually* has the requisite information available to do so).

After reviewing, it is clear that the ERB only partially satisfies the virtuous decision-making qualification. This tells us that the ERB does not appear to currently have access to the information that would be needed to confidently apply my virtue framework to their decision-making process. With this understanding, we can move forward in applying my virtue framework to the VEP in a research capacity to better understand how this information gap theoretically impacts the VEP's ability to perform my ethics-based reflection.

Non-maleficence

In the context of my framework, the virtue of non-maleficence aims to determine whether the ERB makes any software vulnerability retention or dissemination determinations with the intent of causing harm to any citizens of the United States or their social fabric. Since unclassified versions of the annual reports have not materialized (even though the latest VEP charter commits to producing them), we are unable to make an independent determination on this topic that is rooted in the ERB's adjudication data. Our next best option is to turn back to the VEP charter itself, noting again that it states that the VEP's primary focus "is to prioritize the public's interest in cybersecurity and to protect core [information systems] and the U.S. economy through the disclosure of vulnerabilities discovered by the USG."[375] Although this is not the most desirable data point to base a virtue determination on, I do believe it is sufficient to determine that the ERB satisfies the virtue of non-maleficence. Some type of timeseries data that provided a quantifiable trend of past ERB adjudications would have been preferred because (as mentioned in the "Virtue Theory" section) "virtues" are intentional patterns of behavior – and one line from a charter does not fulfill that criterion.

---

[374] White House, 2017, p. 1.

[375] White House, 2017, p. 1.

Again, these virtues only look at the ERB's intent towards the United States, so it is possible that decisions are being made to inflict harm on our adversaries or others external to the United States, but that falls outside the scope of this virtue framework.[376]

Beneficence

In the context of my framework, the virtue of beneficence aims to determine whether the ERB makes their software vulnerability retention or dissemination determinations in such a way that tries to maximize the benefit produced for citizens of the United States and their broader social good. Again, since unclassified versions of the annual reports have not materialized, we are unable to make an independent determination on this topic that is rooted in the ERB's adjudication data. We do know, however, that the ERB is primarily composed of intelligence and law enforcement community members and does not appear to well-represent other stakeholder groups – such as consumers or members of industry – which presents a gap in the ERB's ability to fully reflect on the broader impacts of their decisions on the citizenry. While the idea that the ERB is enhancing the safety of American citizens by furthering national security objectives through their vulnerability adjudications is a relevant component to beneficence, it cannot be the *only* component; we should be cautious to unquestioningly assume that all decisions falling under the umbrella of "national security" are also done so in the air of beneficence (this gets back to the idea discussed earlier in this chapter that virtues must be done consciously and intentionally – not coincidentally). I would argue that in order for the ERB to be consciously and intentionally trying to maximize the benefit produced for citizens of the United States and their broader social good through software vulnerability retention or disclosure, they must have access to information on these key stakeholder groups – and it is not clear that they currently do; one cannot intentionally maximize benefits if an entire group of stakeholders are absent from one's equation. Because of this, I have determined that the ERB only partially satisfies the virtue of beneficence in the context of my framework.

It is worth noting that in order for the ERB to maximize benefits for citizens of the United States and their broader social good through software vulnerability adjudications, the ERB must be considering each new adjudication within the context of all their previous adjudication decisions – particularly their past decisions to retain select software vulnerabilities for exploitation. This is important because even though they may believe that each retention decision will ultimately have a beneficial impact, the unchecked aggregation of software vulnerabilities can unintentionally allow for circumstances leading to the development of exploitations that seriously impact private citizens – circumstances which would not have occurred if the software vulnerabilities had been disseminated for patching instead.

---

[376] Please revisit the "Identification of Virtues" section for an explanation as to why my virtue framework has been scoped to only address the national-level.

Solidarity

In the context of my framework, the virtue of solidarity aims to determine whether the ERB's software vulnerability retention or dissemination decisions are being made with concern for – and in the interest of – the citizens of the United States. This virtue seeks to go beyond simple trust or accountability by asking the question "Does the ERB protect its most vulnerable (meaning its citizens who do not have a seat at the table), even if it requires them to patch one of their most valuable software vulnerabilities?" Again, since unclassified versions of the annual reports have not materialized, we are unable to make an independent determination on this topic that is rooted in the ERB's adjudication data. And – again – the only other data point available to us is the VEP charter stating that its primary focus "is to prioritize the public's interest in cybersecurity and to protect core [information systems] and the U.S. economy through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes."[377] Unfortunately, the virtue of solidarity requires more than an empty commitment; it requires the privileged entity (in this case, the ERB) to demonstrate that commitment through accountability to the vulnerable (in this case, the citizens of the United States). Because we have no other data available to us that would demonstrate the ERB's commitment to making adjudications in the interest of the citizens (and the potential disinterest of their own through the patching of valuable vulnerabilities), I determine that the ERB does not satisfy the virtue of solidarity in the context of my framework.

Situational Fairness

In the context of my framework, the virtue of situational fairness aims to determine whether the ERB is taking the entire context of a scenario into account, and actively identifying and correcting any bias present when making a software vulnerability retention or dissemination decision. This virtue is aimed at ensuring that a truly accurate contextual picture of all sides is presented to the ERB so that they can make the most informed adjudication possible by balancing the potential consequences with the context and feasible options available to them. This virtue is particularly relevant to the VEP because it ensures that *all* contextual stakeholder sensitivities are considered and weighted; this includes any contextual sensitivities related to the United States public, *as well as* the contextual sensitivities related to the intelligence and operational components within the United States that would exploit these software vulnerabilities.

Again, since unclassified versions of the annual reports have not materialized, we are unable to make an independent determination on this topic that is rooted in the ERB's adjudication data; of course, this would be dependent on the reports actually containing substantive data (such as

[377] White House, 2017, p. 1.

information regarding which stakeholder were considered, who represented their equities, etc.) – but still, I cannot make a determination based on non-existent data. Through Annex B ("Equity Considerations") of the VEP charter, however, we can begin to develop an understanding for how much effort is currently put into contextualization. Annex B is divided into "Part 1 – Defensive Equity Considerations," "Part 2 – Intelligence, Law Enforcement, and Operational Equity Considerations," "Part 3 – Commercial Equity Considerations," and "Part 4 – International Partnership Equity Considerations." Part 1 & 2 (which both consider government-oriented equities) are quite extensive and composed of multiple subparts, whereas Parts 3 & 4 are only composed of one bullet each:

- **Part 3 – Commercial Equity Considerations:** "If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG relationships with industry?"[378]
- **Part 4 – International Partnership Equity Considerations:** "If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG international relations?"[379]

This would lead us to believe that government-oriented equities are given considerably more weight and consideration than commercial or international partnership sensitivities. The absence of any citizenry-oriented considerations within Annex B (aside from whether enough consumers will apply a patch to offset harm) is also glaringly evident. Based on the information above – and given that the ERB utilizes Annex B to guide equity considerations and contextualization (although they are not limited to it) – I have determined that the ERB does not currently satisfy the virtue of situational in the context of my framework.

Chapter Conclusion

After applying my virtue framework to the ERB (the VEP's decision-making entity), I determined that the ERB only satisfies one of the four virtues: non-maleficence. This means that while I am confident that the ERB is not intentionally trying to inflict harm on US citizens (*non-maleficence*), I cannot confidently say (1) that they are able to maximize benefits for the citizenry or broader social good (*beneficence*), (2) that their adjudication decisions are being made with concern for – and in the interest of – US citizens (*solidarity*), or (3) that they accurately contextualize the scenarios used to make adjudication decisions (*situational fairness*). Since the ERB was unable to satisfy all four virtues, this suggests that the VEP is currently unable to adhere to ethics considerations that are important to software vulnerability-oriented

[378] White House, 2017, p. 14.

[379] White House, 2017, p. 14.

public policy, which directly impedes its ability to promote longer-term social good through its vulnerability adjudications.

A key reason for this conclusion was that I repeatedly encountered the hurdle of insufficient data – which supports my initial findings from the "virtuous decision-making qualification." The ERB itself in at least two of the four virtues – *situational fairness* and *beneficence* – appears to not currently have access to the information needed to be able to fully reflect on the ethics considerations of those virtues. In the case of situational fairness, the ERB seemingly omits entire stakeholder groups from consideration, and focuses rather on the impacts the software vulnerability adjudications will have on different components of the government. Similarly, in the case of beneficence, the ERB again almost exclusively focuses on the perspectives of different components of the government, while seemingly omitting nearly all representation of public-oriented stakeholders. If the ERB were able to (1) provide the unclassified annual reports that the VEP charter commits to, or (2) provide the public with substantive and meaningful data in some other format (such as brief summaries on trends from prior years) that would help establish trends in the ERB's decision-making, it would not only provide the public with additional data sources to perform their own independent application of my ethics-based framework, but would also help the ERB demonstrate the virtue of solidarity and improve public trust in the VEP as a whole.

Chapter 4: Policy Recommendations & Final Discussion

A theme that has consistently emerged across the previous three chapters – as well as across methods – has been that while the VEP charter may robustly consider the government-oriented equities of zero-day software vulnerability disclosures, there is a deficiency in the VEP's consideration of public or social good-oriented equities.

In Chapter 1, we saw this demonstrated as an incongruence within the design of the charter itself; although the first paragraph of the charter clearly states that "the primary focus of this policy is to prioritize the public's interest in cybersecurity,"[380] that prioritization or concern for the consideration of the public's equities is not reflected in the charter's considerations. This was perhaps most noticeable in the "Equity Considerations" (Annex B) portion of the VEP which robustly outlines government-oriented equities, but only lists meager considerations of industry equities while completely omitting any citizenry-oriented considerations. Those actively involved in the public discourse around the VEP were concerned by the absence of parameters for what constituted a "demonstrable, overriding interest"[381] to retain a vulnerability because without it the public has no way of qualifying what does and does not constitute a valid overriding interest in the eyes of the Equities Review Board (ERB). Perhaps a more practical concern, however, is that the VEP is not enforceable to begin with since it is not codified or has an associated Executive Order or National Security Memo installing some sort of enforcing mechanism, meaning that – regardless – the public entities involved cannot technically be held accountable by any type of internal or external oversight board.

In Chapter 2, this same theme emerged, with interviewees specifically pointing out that the VEP – both in design and practice – placed greater emphasis on government-oriented equities than those of consumer and industry stakeholders (two key segments that make up a considerable portion of the social fabric).[382] At the same time, interviewees made it clear that government-oriented equities – at least those related to intelligence or law enforcement functions – were very well-represented, but that there remained key areas where the VEP could be used in a more strategic manner, such as through leveraging it as a mechanism to drive international norms around software vulnerability exploitation. Interviewees also pointed out, however, that government stakeholders were not the only ones deficient in their consideration of public-oriented equities. Furthermore, interviewees saw both government and industry stakeholders as contributing to the Access-as-a-Service market through either the purchasing of vulnerabilities

[380] White House, 2017b, p.1.

[381] White House, 2017b, p.1.

[382] Please refer to section "Consumer & Industry Equities Should Be Better Represented, but 'How' Is Unclear" of Chapter 2 for a comprehensive discussion of this finding.

for exploitation, or through not paying "going price" for the vulnerabilities in order to be able to patch them – both of which were viewed as avenues that put the general public in a potentially compromised security position.

In Chapter 3, my design and application of a virtue-based ethics framework to the VEP yielded results suggesting that the VEP is currently unable to adhere to ethics considerations that are important to software vulnerability-oriented public policy (which I identified as the virtues of *non-maleficence*, *beneficence*, *situational fairness*, and *solidarity*);[383] this deficiency directly impedes the ERB's ability to promote longer-term social good through vulnerability adjudications – again, findings that align with the same emergent theme from Chapters 1 and 2. Through this application of my virtues-based ethics framework, though, I identified areas where the ERB or the VEP Director can implement updates to the current VEP charter to improve their adherence to important ethics considerations, such as implementing an enforceability mechanism to induce accountability, as well as expanding Annex B to better represent consumer and industry equities.

Based on the findings and gaps highlighted across each method, along with the wide array of views captured, I have developed eleven policy recommendations (discussed below) which fall within three over-arching categories: (1) policy recommendations for the VEP charter, (2) recommendations to improve the performance of the VEP, and (3) a strategic recommendation related to the VEP. While these policy recommendations focus on actions that the Federal Government can take, it should be noted that commercial information technology providers do bear a burden to improve the overall security of their products and services to better protect their consumers; the types of policies or programs that the Federal Government could implement to incentivize this commercial sector action is an area where additional research is needed.

Policy Recommendations for the VEP Charter

The following eight recommendations apply directly to the VEP charter and aim at improving the charter's ability to consider – as well as become more aligned with – public or social good-oriented equities.

1. Infuse Enforceability & Accountability into the VEP Through an Executive Order or National Security Memo

The fact that the VEP charter, as it currently stands, is not technically enforceable is the largest loophole uncovered through this research; since the VEP is not codified, nor does it have an associated Executive Order or National Security Memo, compliance with each aspect of the process is not enforced. While the VEP charter may not be perfect, it definitely moves US cyber

[383] Please refer to section "Identification of Virtues" of Chapter 3 for a comprehensive discussion on how and why these virtues were selected.

policy and how we think about vulnerability exploitation in the right direction – that being a unifying national-level policy that attempts to take both government and public equities into consideration before making a final decision. To ensure that the VEP charter is enforceable and can hold responsible parties accountable for their actions, I recommend that the VEP charter be further formalized through either an Executive Order or unclassified (and publicly released) National Security Memo; of the two, an Executive Order would be preferred since Executive Orders must be published in the federal register and become part of the public domain, whereas National Security Memos can be classified and not released. The use of an Executive Order or unclassified National Security Memo is important because these two mechanisms ensure enforceability and compliance, while still providing the Executive Office with the flexibility needed to adapt to future threats and conditions; the cyber domain evolves rapidly, and formalization of the VEP through codification into a statute would provide a rigid structure that would be difficult to adapt to future needs. This action will also improve public trust in the process in several ways: (1) it provides an enforceability and compliance mechanism that demonstrates the US Government's commitment to handling software vulnerabilities in a particular way; (2) it adds an additional layer of transparency that currently does not exist (both the classified and unclassified annual reports mentioned in the charter must now materialize, providing a foundation for external oversight and assessment); and (3) an Executive Order or unclassified National Security Memo supports the VEP's longevity and ensures that it will not fall dormant (as we saw happen with its first iteration in 2010).

In the context of my virtue-based ethics framework, the accountability resulting from the addition of an enforcement mechanism is one component that would help the ERB satisfy the solidarity virtue. Through the addition of an enforcement mechanism, the ERB demonstrates its willingness to hold itself and all other responsible parties accountable to the public for their actions.

2. Begin Producing the Classified & Unclassified Annual Reports as Soon as Possible, and Clarify What Should Be Included in Said Reports

The current VEP charter commits to providing both classified and unclassified annual reports; my research provided limited evidence that suggests the classified reports are being produced for Congress, with conclusive evidence that the unclassified reports are not materializing. I recommend that these reports – both the classified and unclassified version begin being produced as soon as possible (as determined by the VEP Director) to (1) provide a source of data to guide other US Government decisions that may be improved by having access to said data, and (2) increase public trust in and transparency into the way the US Government handles vulnerability related decisions.

I also recommend that section 4.3. ("Annual Reporting") of the VEP charter (1) be revised to outline a minimum set of data or information (e.g., summaries) required to be included in the unclassified report specifically (which will ensure that these unclassified reports are substantive

in nature), and (2) clarify what constitutes a "demonstrable, overriding interest" for vulnerability retention. Without successful production of these reports or an understanding of what is and is not considered a legitimate reason for vulnerability retention, there is no objective way to determine how appropriate the ERB's adjudication decisions are, or if they truly are prioritizing disclosure over retention (as is declared in the charter).

In the context of my virtue-based ethics framework, the unclassified reports (assuming that they include substantive and meaningful data that establish trends in the ERB's decision-making) are another component that would help the ERB satisfy the solidarity virtue. Through the publication of meaningful reports, the ERB demonstrates its willingness to hold itself and all other responsible parties accountable to the public for their actions.

3. Improve Consumer & Industry Representation During ERB Discussions by Expanding Annex B & Considering the Implementation of an "Additional Representation Mechanism"

The research conducted throughout this study – including both the open-source research of the VEP, as well as VEP SME interviews – all provide evidence to support the claim that the equities of consumers and industry (and by extension, the general public) are currently not being adequately represented during ERB vulnerability adjudication discussions. The design of the VEP itself is flawed in that it only robustly considers the equities of the intelligence and law enforcement communities – and this is most evident in the ERB composition (given that the majority of ERB members are affiliated with the intelligence or law enforcement community) and the layout of Annex B ("Equity Considerations") (which thoroughly considers US Government-oriented equities, but almost entirely omits the equities of the US citizenry and industry).

In order to overcome this design flaw and improve consumer and industry representation, I recommend that, at a minimum, Annex B ("Equity Considerations") of the current VEP charter be expanded to provide ERB members with a guide to support robust consideration of consumer and industry equities; this recommendation allows for improved representation without overly burdening the ERB or adjudication process. To achieve this, Part 3 of Annex B should be expanded to provide a more robust representation of industry equities, and a new section should be established within Annex B (e.g., Part 5) to provide a robust representation of equities tied to the general US citizenry; I suggest referencing "The Importance Of Ethics In An Increasingly Digital Society," "Social Good," and "Virtue Theory" sections of Chapter 3 to support the VEP Director in understanding the importance of this new addition and guide its development.

In addition to this minimum requirement, I recommend that an additional representation mechanism or effort for consumers and industry be put in place to ensure that their equities are considered. My "Interview Results" section of Chapter 2 outlines five potential formats for this

"additional representation mechanism;"[384] I would recommend that the VEP Director (or the party delegated the responsible for identifying and implementing this "additional representation mechanism" by the VEP Director) begin by reviewing the five formats indicated there, as they represent the aggregated formats identified by the VEP SMEs I interviewed.

In the context of my virtue-based ethics framework, the expansion of Annex B is a component that would help the ERB satisfy both the beneficence and situational fairness virtues. By providing ERB members with a guide to support the robust consideration of consumer and industry equities, they have increased access to information on these stakeholder groups and any associated contextual sensitivities which they can then use to try to maximize benefits for these groups through their adjudication decisions.

4. Expand "Part 4" of Annex B to Address Internationally Oriented Equities

While the VEP is meant to be nationally-facing – that is, that its main objective is to assess the potential impacts of software vulnerabilities on the US citizenry and other national security priorities – the resulting adjudication decisions do hold potential ramifications for the broader international community. This fact is acknowledged by the VEP through the inclusion of the States Department on the ERB, as well as through Part 4 of Annex B which looks at how US Government international relations may be impacted by the retention or dissemination of newly discovered software vulnerabilities. The results of my VEP SME interviews, however, suggested that there are two key flaws with this current design: the interview results support the claim that (1) a robust perspective on how vulnerability adjudications will impact our international partnerships is currently not present in the ERB, and (2) there is no consideration given to how vulnerability adjudications may potentially impact other civilian members of the international community (e.g., how the retention of a vulnerability may put pro-democracy civilians from other countries [such as journalist] in danger). To address this gap, I recommend expanding Part 4 of Annex B to guide ERB discussions in a way that more robustly considers the impact of ERB adjudication decisions on the international community (that is, on both our formal international partnerships, as well as our informal relationship to other members of the international community). This solution would ensure that an additional layer of thought is placed into the adjudication process as it relates to international implications (i.e., as to not be entirely reliant on the State Department) without overly burdening the VEP.

5. Provide Definitions or Parameters Within the Charter That Outline What Constitutes a "Demonstrable, Overriding Interest" for Vulnerability Retention

While the VEP charter states that it prioritizes the public's interest in cybersecurity, this prioritization is linked to a caveat: "absent a demonstrable, overriding interest in the use of the

[384] Refer to the "Consumer & Industry Equities Should Be Better Represented, but 'How' Is Unclear" section of Chapter 2.

vulnerability for lawful intelligence, law enforcement, or national security purposes."[385] One gap present within the charter is the detailing of what constitutes a "demonstrable, overriding interest." I do not expect the VEP to list very specific examples given that this is an unclassified document, but I do recommend that it be revised to provide some structure as to what is (or is not) considered a valid overriding interest. Providing no guidance or information not only weakens public confidence (i.e., those active in public discourse on this topic, such as digital advocacy groups and select private sector companies) in this particular aspect of the charter, but it also undermines the ERB's accountability – especially if the Executive Office were to accept my first recommendation and formalize the VEP via an Executive Order or National Security Memo; if a minimum standard or threshold of what constitutes an overriding interest is not established, then there is no way to enforce or ensure that the threshold of "overriding interest" is in fact being appropriately fulfilled and met with consistency.

6. Provide Insight into How Non-ERB Members Are Notified to Claim Equity in a Vulnerability Under Review

As outlined in Chapter 1, all vulnerability adjudication discussions include the ten permanent ERB members, as well as the agency or department that identified the zero-day software vulnerability (if said department is not one of the permanent ERB members). In addition, the VEP charter states that "other [US Government] agencies may participate [in the vulnerability adjudication discussions] when demonstrating responsibility for, or identifying equity in, a vulnerability under deliberation."[386] However, the charter does not discuss how or through what channels non-ERB members are notified of a vulnerability under review: if a department does not know that a vulnerability that may impact them or their stakeholders is under review, how can they claim equity and attend the deliberations? This is a potentially significant gap when discussing equities; if there is no process in place to ensure that every agency or department who may have equity in a vulnerability is notified and given the opportunity to have their equities considered during the adjudication process, then we have identified a flaw in the charter's design through which certain stakeholders' equities may be going overlooked.

It is possible that there are already formal processes or channels in place to address this potential gap; if so, I recommend that the VEP charter be updated to include this information (or as much detail as possible if the formal process is sensitive or classified) to help eliminate the perceived existence of a gap in the policy. If a formal process for notifying departments who may have equity in a vulnerability going through ERB review is not currently in place, I recommend one be established; again, this is crucial to ensuring that all stakeholders' equites are being considered prior to a vulnerability adjudication. Once in place, the VEP charter should be updated to reflect this information.

---

[385] White House, 2017b, p. 1

[386] White House, 2017b, p.3.

7. Provide More Defined Handling & Follow-On Processes to Support Expeditious Vulnerability Remediation

Along similar lines as recommendation #5, the "Handling & Follow-On Actions" section of the VEP charter is rather vague, lacking sufficient structure to be able to hold ERB members accountable; an example of this vagueness is the disclosure guidelines currently provided: "Disclosure of vulnerabilities submitted for equity review will be conducted according to agreed-upon guidelines that are consistently and responsibly followed by all members."[387] For this section of the VEP charter, I make the following recommendations:

- **Set a more defined timeline allowed for vulnerability disclosures after a dissemination decision has been made:** The current charter states "dissemination will be made in the most expeditious manner and when possible within 7 business days."[388] Instead, this timeline should be defined in a way that sets a limit on the maximum duration of time the notifier can go without notifying the applicable vendor (e.g., "dissemination will be made in the most expeditious manner possible, but within no less than 7 business days of a dissemination decisions.").
- **The disclosure guidelines should be established within the charter to ensure consistency:** As previously mentioned, the current disclosure guidelines within the VEP charter are vague. This can not only compromise consistency in decision-making, but also makes it difficult to hold ERB members accountable; if the guidelines are not included within the charter for the public to view, then the public is unable to hold ERB members accountable to them. As such, I recommend that this section of the charter be fleshed out to include a more structured outlining of what the vulnerability disclosure process should look like, including the associated timelines within which each step should be accomplished.
- **Set a more defined process, expectations, and timeline for the vendor follow-up:** Currently, the charter states the following as the follow-up protocol: "the releasing agency is expected to follow-up so the ERB can determine whether the vendor's action meets USG requirements." This single-sentence statement does not provide enough information to adequately guide notifiers, nor does it provide adequate information to be able to hold the responsible parties accountable. As such, I recommend that: (1) a finite duration of time be included within which the notifying entity is required to follow-up with the ERB (e.g., "the releasing agency is expected to follow-up so the ERB within 20 business days"); (2) the actual (or a summary of) the US Government requirements that vendors are expected to achieve should be included in the charter to support the ERB in consistently determining whether the vendor has in fact met the relevant requirements (e.g., timeframe within which a patch is expected to be developed); and, (3) outline what constitutes "other mitigation steps" that the US Government is able to take if a vendor

[387] White House, 2017b, p. 8.

[388] White House, 2017b, p. 8.

fails to respond adequately (it is understandable that all mitigation steps may not be listable given the unclassified nature of this document, but some representation of what the government is prepared to do should be included).

8. Add a New "Annex D" That Includes the Virtue-Based Ethics Framework Developed in This Dissertation to Guide ERB Ethics Considerations

The application of my virtue-based ethics framework to the ERB (the VEP's decision-making entity) in Chapter 3 indicated that the VEP is currently unable to adhere to ethics considerations that are important to software vulnerability-oriented public policy,[389] which directly impedes its ability to promote longer-term social good through its vulnerability adjudications. Along with this key finding, I identified areas where the ERB or VEP Director could focus charter updates to improve this metric, and have infused them into specific recommendations above (e.g., such as the expansion of Annex B in recommendation #3). Another means of achieving this, however, is by including my virtue-based ethics framework into the VEP charter under a new "Annex D." This new addition would provide two key benefits. The first is that the VEP Director and ERB could use the new Annex D going forward to perform self-assessments utilizing the full gamut of classified data; this would provide the VEP Director and ERB with more contextualized findings regarding their adherence to ethics considerations, along with more tailored solutions on how to guide updates to the process to increase their promotion of social good. Second, if my virtue-based ethics framework is implemented by the VEP Director and is also included under a new Annex D, its inclusion would increase transparency by providing public insight into how the VEP Director and ERB gauge their adherence to ethics considerations to promote social good.

Recommendations to Improve the Performance of the VEP

The following two recommendations aim at improving the performance of the VEP, some through direct application to the charter, and others through tangential applications that – in the long run – would benefit the overall VEP process.

1. An Additional Policy Outside of the VEP Should Be Put in Place That Focuses on the Purchasing of Vulnerabilities & Exploits

This research highlighted conversations around the US Government's purchasing of vulnerabilities and exploits as a means of achieving certain ends – whether for information gathering or operational purposes. One key concern voiced within the literature regarding this topic is the fact that vulnerabilities or exploits that are purchased are exempt from review by the VEP due to associated Non-Disclosure Agreements (NDAs) (viewed as a loophole by many

[389] Please refer to the "Identification of Virtues" section of Chapter 3 for a comprehensive discussion on this topic.

within the media and digital advocacy groups), as well as additional concerns regarding the role the government is playing in fueling the Access-as-a-Service Market as a result of these purchases.[390] On the other side of this argument, however, are legitimate national security reasons linked to the continued purchasing and use of such vulnerabilities. Although both sides of this argument have valid reasons and concerns, the VEP and ERB meetings are not the appropriate venues for making decisions on this topic; that is not the objective of the VEP, and therefore the VEP is not appropriately postured to make the most informed decision. Acknowledging the importance and timeliness of this concern, however, I recommend that the US Government develop an additional stand-alone policy that establishes the US Government's official stance on the appropriate parameters around the purchasing and use of third-party vulnerabilities and exploits; this stance may or may not be enforceable (as we see with the current VEP charter), but it would help clarify the appropriate use of such services by the US Government. I acknowledge the intricacies and complexities associated with developing such a policy (particularly given the intermingling of private sector ventures and government intelligence gathering), but just because it is difficult does not mean we should not try; the Access-as-a-Service market is not going away, and proper steps should be taken to protect the vulnerable. Although this might not aid in the regulation of these services, it will help establish applications deemed unacceptable (e.g., the purchasing of an exploit to gain access to a private citizen's devices or network without appropriate legal impetus).

2. The VEP Should Remain Focused on Software Vulnerabilities

Given that the cyber domain will continue to evolve and present new challenges to the US, it is important that the VEP remain focused on software vulnerabilities and not be required to expand their scope of review to other types of technology or technology application. This includes not expanding the VEP to review discussions on specific Tactics, Techniques, and Procedures (TTPs) used in conjunction with zero-days, but rather remaining focused on the risk presented by a zero-day itself.

Strategic Recommendations Related to the VEP

The following recommendation aims to use the VEP in a strategic manner outside of its current scope. It is not intended to be applied directly to the current VEP charter, but rather looks to leverage the charter as a template.

[390] Please reference the "Interview Results" section of Chapter 2 for more information around this discussion.

1. The US Government Should Actively Engage Other Countries in Designing & Implementing Their Own VEPs

As expressed throughout this research, the world is going through a pivotal time of cyber domain development (both in terms of technological advancements and maturing of tactics to maneuver within and manipulate said domain), including how we as humans interact with that world. Simultaneously, the distribution of power around the globe in also evolving, resulting in a threat landscape that requires a multi-faceted approach to countering. As part of a broader approach, I recommend that the US Government use its unique position and experience in the cyber domain to educate and work with our partners and other countries to develop their own VEP-like policies as a way to influence cyber norms in a direction that is beneficial to the US. The findings from my VEP SME interviews suggests that other countries are looking to the US for such guidance, and there are several reasons – both strategic and practical – for us to provide more active support on this front.[391]

Study Assumptions & Constraints

This study was conducted on the foundation of three core assumptions. The first assumption is that the VEP charter published in 2017 is the most up-to-date version – meaning that there have not been any updates or changes made to this version of the charter outside of the public's knowledge. The second assumption is that the classified Annex C mentioned in the charter, which is supposed to outline vulnerabilities that are exempt from the VEP's review, does in fact exist. And the third assumption is that all ERB members do in fact have access to the information or resources that the VEP charter claims they have access to throughout the adjudication process.

With these assumptions in mind, I identified three key constraints on this study. The first and perhaps most impactful constraint is that I only reviewed unclassified resources for this study; this constraint extends to my interviews as well, which were all conducted at the unclassified level. The decision to conduct this entire study at the unclassified level was a deliberate one. As I began my open-source review for information on the VEP, it became clear that there was a lack of publicly available data. The only primary sources available were the original and current VEP charters, and a small number of public statements made by government officials. This meant that the sizeable volume of secondary sources on the VEP were largely rooted in opinion, limiting the amount of objective analysis that could be done. By conducting this study completely at the unclassified level, all the information within it is now available to the public.

The second constraint is that with no publicly available VEP annual reports or other methods-based examinations of the VEP, there is no other available body of rigorous findings to compare my results to. The third constraint is linked to the limited number of countries with VEP policies in place. Due to the very small number of other countries with publicly acknowledged

[391] Please reference the "Interview Results" section of Chapter 2 for more information around this discussion.

and accessible VEP charters – and given that the applicable charters were almost identical – there was no robust means for me to assess how the US VEP charter compares to those of other countries and potentially identify elements of other VEP charters that the US VEP charter may not include. This means that the findings of this study are, at best, only generalizable to other anglospheric or western countries, and is for all intents and purposes an American-focused study.

While the findings of this study are subject to the assumptions and constraints outlined above, they provide a new foundation of objectively generated information and create a basis for future research.

Future Research

This study highlighted several areas where additional research is needed. The policy community is in need of more objective and rigorous methods-based examinations of the VEP (and similar policies) to better inform the revision of current and development of new cyber-oriented public policies. While there is a plethora of recommendations rooted in uninformed opinion, these cannot be used to shape the future of cyber policy in the United States.

An exploration into what the impact of the VEP has been is another key area where additional research is needed. What type of downstream effects has the VEP created? In what ways has the VEP generated "good" or beneficial outcomes for society, and in what ways has it generated "bad" or undesirable outcomes? We know through public reporting that the VEP has led to the capture of varying types of cybercriminals, but at what costs or possible infringements of civil liberties? Questions like these have not been addressed in an objective or methods-based manner and would provide the research community with a deeper understanding into the potential tradeoff between benefits and civil liberties which could greatly inform the structure of cyber-oriented public policies in the United States going forward.

The type and amount of data required to make more informed decisions at the federal level regarding software vulnerabilities is another area where additional research is needed. This is particularly true for better understanding the prevalence and impact of a given software vulnerability, as well as the development of new tools to support these assessments.

I also hope this study sparks new interest into the development and application of ethics frameworks to cyber-oriented public policies – an area that is deeply under-researched. My research indicated that policies oriented towards artificial intelligence and machine learning have been the primary focus of ethics application – leaving the majority of cyber policies unexamined and unaccounted for from an ethics perspective. Further research applying ethics frameworks to non-AI / non-ML public policies is needed to ensure that this growing segment of public policy geared towards the cyber or digital domain adequately reflects the ethics considerations deemed foundational to society.

Closing Remarks

My research into the VEP highlighted a heated debate around the use software vulnerabilities that – although not always happening in the view of the public – is alive and well. While there are digital rights and privacy advocates who argue that the US Government should disclose any and all newly discovered software vulnerabilities for immediate patching, we need to remain firmly rooted in the reality of the world we live in. This requires acknowledging the uncomfortable truth that having a "default to disclosure" federal policy around zero-day software vulnerabilities would not necessarily be in the best interest of US national security priorities or in the best interest of the American public. There are scenarios in which the retention of a vulnerability for either intelligence gathering or operations is in fact justified and necessary, and we should remain sensitive to these situations and protect the associated vulnerabilities. With that said though, we should not subscribe to a blanket policy of vulnerability retention and stockpiling; we know that this too is dangerous, irresponsible, and counterproductive to national security and public interests. Ensuring that we are guided by a structure that is not overly biased towards either intelligence community or disclosure is key.

In response, the VEP was developed as a means to formalize and guide the balancing of the practical and strategic risks and benefits associated with the retention of software vulnerabilities in a consistent and repeatable way. Although not perfect, the VEP brought together different components of the Federal Government that were responsible for different aspects of national security, and did so in a way that was substantially more transparent and structured than any other comparable policy in the world at the time of its public release. Even to this day it remains the foundation from which other countries have built their own Vulnerabilities Equities Processes. Still, there are areas where the current VEP could be improved; items like ensuring public reporting of past adjudication decisions to improve transparency or incorporating ethics-based components are key to building public confidence and trust in the Federal Government's handling of such closed-door activities.

The VEP is not just a procedural document though. It serves a fundamental purpose of pushing US cyber policy in a direction that we as a country deem correct, forcing us to think about the influence that we as a global power – both in the governmental and economic sense – want to effect on the broader international community: How do we want vulnerabilities and cybersecurity to be thought and spoken about, and what kind of example are we as a country setting? How vulnerable are our allies to specific bugs, and should that stop us from leveraging said vulnerabilities if our allies knowingly invest in technology that could be vulnerable? There will always be competing equities, and there will be times the US Government needs to exploit a vulnerability for national security or significant law enforcement efforts, but the VEP forces the Federal Government to look at the other types of harm that they might cause through the retention and exploitation of a vulnerability. There is no VEP structure that will ever be able to hold the weight of every criticism – it is simply not possible – but if our goal is to conceptualize

and implement a VEP that maximizes the amount of societal good produced while minimizing the amount of harm inflicted, moving both government and industry in a direction that builds a less-vulnerable cyber ecosystem, then it is an effort that is worthwhile.

In its current state, the VEP charter assumes that the equities considerations around "public interest" and "public good" are satisfied by (1) the key stakeholders written into the vulnerability adjudication process, and (2) the range of equities considered in Annex B – both of which are primarily representative of the intelligence and law enforcement communities. My research, however, found that this assumption is not true. There is an expansive body of literature in the social sciences that indicate there are several other social considerations that can and should be represented to robustly consider the impact of policy decisions on broader public good. It is in this area at the nexus of the cyber domain and public policy that we as a society should begin re-examining what equities we think need to be included in public policy decisions, how we expect those equities to be represented, and whether there are other public policies that should be re-examined and updated to better reflect these social equities.

Appendix A: VEP Interview Protocol

The following section outlines the interview protocol used during my interviews with Vulnerabilities Equities Process (VEP) subject matter experts (SMEs). The final interview protocol, all associated procedures (e.g., initial interview outreach, material safeguarding, etc.), and overall study design were submitted to RAND's Human Subjects Protection Committee (HSPC) for review and approval prior to beginning engagement with any VEP SMEs. This study was approved and determined to be a "Category 2—Educational Tests, Survey Procedures, Interview Procedures and Observation of Public Behavior" study by RAND's HSPC and was deemed exempt from any further review. For verification, contact RAND's HSPC and reference Study 2021-N0313. Interviewees were informed at the beginning of each interview that the interview discussion and resulting content needed to remain at the unclassified level, that their identity would not be revealed (neither directly nor indirectly), and that quotes from our discussions would be published. The following interview protocol lists the questions used during these semi-structured interviews.

Introduction

- What was your relationship to the VEP?
- When casting a dissemination decision vote, do you think ERB members tend to cast votes in a way that leans more towards their Intelligence or Law Enforcement Communities' equities? Or for the most part do you think they vote objectively each time?

Regarding the Process

- The VEP makes a commitment to publish annual reports with metrics (both a classified and unclassified version), but I haven't been able to find one. Do they exist? And if so, where can the public access them?
- The VEP still has not been codified into law. With the new level of transparency included in the latest iteration, do you feel it is still necessary to have the VEP codified as an enforceability and compliance mechanism (for both the government and the public), or is that no longer necessary?
- Do you believe that NDAs, partner agreements, and deeming work as "sensitive operations" are actively used as loopholes to avoid VEP review?
- The NSA's retention of the VEP Executive Secretariat role (although it is mainly an administrative function) received sharp criticism – many saying it presented a conflict of

interest. Do you think the NSA holding this position is a problem? If so, who would be better suited to hold this function (e.g., DHS) and why?
- Is there anything else that the current VEP charter should be considering? If we envision a more comprehensive vetting process, what would / should it look like?

Regarding Consumer & Industry Equities

- A majority of the VEP Equities Review Board members are associated with either the IC or LE (e.g., DoD, DHS, DoJ),[392] and there is a notable lack of involvement of elected representatives, members of the private sector, or an entity that focuses on civilian consumer security and protection – all of which would be appropriately postured to represent the interests of citizens. Do you think this perceived imbalance is truly an issue and introduces bias into the VEP decision-making process? Or do civilian consumers currently have their equities adequately considered?
- Even if a vulnerability is disclosed, how much of a concern is it that (1) the respective vendor will *not* develop a patch, and (2) that – once developed – the applicable consumers will *not* apply the patch?
- The VEP charter does not really include private sector involvement. Should there be more participation by the private sector? And if so, what do you think that should look like? ((Are there rules or limitations around if / how members of the VEP can engage the private sector?))

Looking Forward

- In your opinion, should the VEP be broadened to consider more than just software vulnerabilities, such as any other specific cyber programs, tactics, or techniques, and applications? (e.g., law enforcement or government use of facial recognition) Could this also be applied to corporate entities who engage in similar behaviors? (e.g., consumer behavior tracking, ad targeting)
- Should the VEP decision-making process include more of an international perspective? (e.g., include a Five Eyes representative, etc.)
- What about expanding this into a "world VEP" or global set of equities & considerations? Would this be possible, or even useful?

Closing

- Are there any other issues that I didn't ask about that you think are key to the VEP process, transparency, or decision making?

---

[392] See Appendix B for a breakdown of which VEP ERB members are associated with either the IC or LE.

- Is there anyone else you recommend I speak with about this topic?

Appendix B: VEP Equity Review Board Members' IC or LE Association

This section lists all ten members of the Vulnerabilities Equities Process' (VEP) Equity Review Board (ERB) and indicates whether they are associated with the intelligence community or law enforcement. Understanding an ERB member's association provides insight into the types of equities they may be more concerned about. The table below indicates an overwhelming representation of intelligence community and law enforcement associated equities, and – just as importantly – highlights the marginalized representation of non-intelligence community or law enforcement equities.

Table 3: VEP Equity Review Board Members' IC or LE Association

VEP ERB Member	Intelligence Community	Law Enforcement	Neither
Central Intelligence Agency	X		
Department of Commerce			X*
Department of Defense (including the National Security Agency (NSA) (including Information Assurance and Signals Intelligence elements)), United States Cyber Command, and DoD Cyber Crime Center (DC3))	X		
Department of Energy	X		
Department of Homeland Security (to include the National Cybersecurity Communications and Integration Center (NCCIC) and the United States Secret Service (USSS))	X	X	
Department of Justice (to include the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force (NCIJTF))	X	X	
Department of State	X	X	
Department of the Treasury	X	X	
Office of the Director of National Intelligence (to include Intelligence Community-Security Coordination Center (IC-SCC))	X		
Office of Management and Budget			X

SOURCE: White House, 2017b.; Office of the Director of National Intelligence, n.d.
*Note: Although the Department of Commerce does have law enforcement-oriented components, the idea of economic development and prosperity is more central to their mission and is likely more prominent in their equities discussions. For this reason, I have associated the Department of Commerce with "Neither."

References

115th Congress, *Cyber Vulnerability Disclosure Reporting Act*, H.R.3202, July 12, 2017a. As of October 2020: https://www.congress.gov/bill/115th-congress/house-bill/3202/text?q=%7b%22search%22%3A%5b%22jackson+lee%22%5d%7d&r=1

115th Congress, *Protecting Our Ability to Counter Hacking (PATCH) Act of 2017*, H.R.3202, May 17, 2017b. As of October 2020: https://www.congress.gov/bill/115th-congress/house-bill/2481

50 U.S. Code § 3316a, *Reports on intelligence community participation in vulnerabilities equities process of Federal Government*, December 20, 2019. As of October 2020: https://www.law.cornell.edu/uscode/text/50/3316a

AccessNow, *A Human Rights Response To Government Hacking*, September 2016. As of October 2020: https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf

Adams, P., "Ethics with character: Virtues & the ethical social worker," *Journal of Sociology & Social Welfare*, Vol. 36, 2009, pp. 83-105.

Agence Nationale de la Sécurité des Systèmes d'Information, "The French CIIP Framework," Government of France, n.d. As of October 2020: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/

Aitel, Dave, & Matt Tait, "Everything You Know About the Vulnerability Equities Process Is Wrong," *Lawfare*, August 18, 2016. As of November 2020: https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong

Aldrich, Richard J., & John Kasuku, "Escaping from American intelligence: culture, ethnocentrism and the Anglosphere," *Royal Institute of International Affairs*, Vol. 88, No. 5, September 2012, pp. 1009-1028. As of December 2021: https://www.jstor.org/stable/pdf/23325014.pdf?refreqid=excelsior%3A789eb223e4ebf96bea77e7f4b19b0299

Ambastha, "Taking a Hard Look at the Vulnerabilities Equities Process and its National Security Implications," *Berkeley Technology Law Journal*, April 2019. As of October 2020: https://btlj.org/2019/04/taking-a-hard-look-at-the-vulnerable-equities-process-in-national-security/

Annas, Julia, "Virtue Ethics," *The Oxford Handbook of Ethical Theory*, 2007. doi: 10.1093/oxfordhb/9780195325911.003.0019.

Aristotle, *Basic Works of Aristotle*, ed. Richard McKeon, trans. C.D. Reeve, Penguin Random House, New York 2001, XI–XVIII, n.d.

Australian Signals Directorate, "About ASD," Government of Australia, n.d.a. As of October 2020: https://www.asd.gov.au/about

Australian Signals Directorate, "Responsible Release Principles for Cyber Security Vulnerabilities," Government of Australia, n.d.b. As of October 2020: https://www.asd.gov.au/publications/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities

Awojana, T., & T.S. Chou, *Overview of learning cybersecurity through game based systems, Conference Proceedings,* New Orleans: Conference for Industry and Education Collaboration, 2019.

Banks, S., & A. Gallagher, *Ethics in professional life: Virtues for health & social care*, London, England: Palgrave Macmillan, 2009.

Baras, John S., Jonathan Katz, & Eitan Altman, eds., *Decision and Game Theory for Security, Conference Proceedings*, College Park: Second International GameSec Conference, 2011.

Bartlett, R. C., "Socratic political philosophy & the problem of virtue," *American Political Science Review*, Vol. 96, 2002, pp. 525–533.

Bhattacherjee, Anol, "Social Science Research: Principles, Methods, and Practices," in Bill Pelz (ed.), *Research Methods for the Social Sciences*, n.d. As of December 2021: https://courses.lumenlearning.com/suny-hccc-research-methods/chapter/chapter-9-survey-research/

Booth, Alison, "Firefox users left feeling vulnerable as judge keeps Tor hack under wraps," *Naked Security*, May 2016. As of October 2020: https://nakedsecurity.sophos.com/2016/05/19/firefox-users-left-feeling-vulnerable-as-judge-keeps-tor-hack-under-wraps/

Bradford Franklin, Sharon, The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes, 2019. As of November 2020: https://docs.wixstatic.com/ugd/c28a64_d67e649778704af09b10d32fad27b317.pdf

Braga, Matthew, "When do Canadian spies disclose the software flaws they find? There's a policy, but few details," *CBC*, September 6, 2017. As of October 2020: https://www.cbc.ca/news/technology/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007

Braun, V., & V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, Vol. 3, 2006, pp. 77-101. doi:10.1191/1478088706qp063oa

Brewer, John D., & Robert L. Miller, (eds.), *The AZ of social research: a dictionary of key social science research concepts*, SAGE Publications, 2003.

Brewster, Thomas, "Cyber Weapons Dealer Investigates 'Leak' Of Tor Hack That Helped Cops Bust Child Porn Site," *Forbes*, December 2016. As of October 2020: https://www.forbes.com/sites/thomasbrewster/2016/12/02/exodus-intel-the-company-that-exposed-tor-for-cops-child-porn-bust/?sh=5f1c6b485f8c

British Academy & Royal Society, "Data Management and Use: Governance in the 21st Century," 2017.

Burr, Christopher, Mariarosaria Taddeo, & Luciano Floridi, "The Ethics of Digital Well-Being: A Thematic Review," *Science and Engineering Ethics*, Vol. 26, 2020, pp. 2312-2343. As of October 2021: https://doi.org/10.1007/s11948-020-00175-8

Burt, Tom, "New nation-state cyberattacks," Microsoft, March 2021. As of December 2021:

Calvo, Rafael A., & Dorian Peters, "Promoting Psychological Wellbeing: Loftier Goals for New Technologies," *IEEE Technology and Society Magazine*, Vol. 32, No. 4, 2013, pp. 19-21. As of October 2021: https://ieeexplore.ieee.org/abstract/document/6679310

Carnegie Endowment for International Peace, "International Policy Conference on Government Vulnerability Management [Event]," 2018. As of October 2020: https://carnegieendowment.org/2018/12/05/international-policy-conference-on-government-vulnerability-management

Castleberry, Ashley, & Amanda Nolen, "Thematic analysis of qualitative research data: Is it as easy as it sounds?," *Currents in Pharmacy Teaching and Learning*, Vol. 10, No. 6, June 2018, pp. 807-815. As of December 2021: https://www.sciencedirect.com/science/article/pii/S1877129717300606

Center for Cyber Security, "CCB Coordinated Vulnerability Disclosure Policy," Government of Belgium, n.d. As of October 2020: https://ccb.belgium.be/en/vulnerability-policy

Center for Internet and Society, *Government Hacking: Vulnerabilities Equities Process [Event]*, Stanford Law School, 2016. As of October 2020: http://cyberlaw.stanford.edu/events/government-hacking-vulnerabilities-equities-process

Charlet, Kate, Sasha Romanosky, & Bert Thompson, "It's Time for the International Community to Get Serious about Vulnerability Equities," *Lawfare*, November 15, 2017. As of November 2020: https://www.lawfareblog.com/its-time-international-community-get-serious-about-vulnerability-equities

Charmaz, Kathy, "Grounded Theory as an Emergent Method," in Sharlene Nagy Hesse-Biber & Patricia Leavy (Eds.), *Handbook of Emergent Methods*, 2008. The Guilford Press.

Christian, Paula, “Franklin man sentenced to 9 years after caught up in notorious FBI child porn operation,” Channel 9 WCPO Cincinnati, March 2019. As of October 2020: https://www.wcpo.com/news/i-team/franklin-man-sentenced-to-9-years-after-caught-up-in-notorious-fbi-child-porn-operation

Cimpanu, Catalin, “US Cyber Command starts uploading foreign APT malware to VirusTotal,” *ZDNet*, November 2018. As of December 2021: https://www.zdnet.com/article/us-cyber-command-starts-uploading-foreign-apt-malware-to-virustotal/

Clark, M. J., *The vision of Catholic social thought: The virtue of solidarity & the praxis of human rights*, Minneapolis, MN: Fortress Press, 2014.

Collier, Kevin, “From offense to defense: NSA's Microsoft flaw alert shows shift in public strategy,” *EuroNews*, January 2020. As of October 2020: https://www.euronews.com/2020/01/14/offense-defense-nsa-s-microsoft-flaw-alert-shows-shift-public-n1115456

Computer Incident Response Center, “Responsible Vulnerability Disclosure,” Government of Luxemburg, n.d. As of October 2020: https://www.circl.lu/pub/responsible-vulnerability-disclosure/

Computer Security Resource Center, “Comprehensive National Cybersecurity Initiative (CNCI),” NIST, June 2016. As of December 2021: https://csrc.nist.gov/Topics/Laws-and-Regulations/executive-documents/CNCI

Constantin, Lucian, “TrickBot explained: A multi-purpose crimeware tool that haunted businesses for years,” *CSO*, December 2020. As of May 2021: https://www.csoonline.com/article/3600457/TrickBot-explained-a-multi-purpose-crimeware-tool-that-haunted-businesses-for-years.html

Council on Foreign Relations, “As Germany Moves Toward a More Offensive Posture in Cyberspace, It Will Need a Vulnerability Equities Process,” September 2018. As of October 2020: https://www.cfr.org/blog/germany-moves-toward-more-offensive-posture-cyberspace-it-will-need-vulnerability-equities

Cox, Joseph, “The FBI May Be Sitting on a Firefox Vulnerability,” *Motherboard*, Vice, April 2016a. As of May 2021: https://www.vice.com/en/article/aekeq4/the-fbi-may-be-sitting-on-a-firefox-vulnerability

Cox, Joseph, “The FBI Used a 'Non-Public' Vulnerability to Hack Suspects on Tor,” *Motherboard*, Vice, November 2016b. As of May 2021: https://www.vice.com/en/article/kb7kza/the-fbi-used-a-non-public-vulnerability-to-hack-suspects-on-tor

Creswell, J. W., “Research Design: qualitative & quantitative approaches,” 1994, SAGE Publications.

Crocker, Andrew, "Time Will Tell if the New Vulnerabilities Equities Process Is a Step Forward for Transparency," *EFF*, November 16, 2017. As of December 2020: https://www.eff.org/deeplinks/2017/11/time-will-tell-if-new-vulnerabilities-equities-process-step-forward-transparency

CrowdStrike, “What is a botnet?,” August 2020. As of December 2021: https://www.crowdstrike.com/cybersecurity-101/botnets/

CYBERCOM_Malware_Alert, User Profile, n.d. As of December 2021: https://www.virustotal.com/gui/user/CYBERCOM_Malware_Alert

Cybersecurity & Infrastructure Security Agency, “CISA Coordinated Vulnerability Disclosure (CVD) Process,” n.d. As of October 2020: https://www.cisa.gov/coordinated-vulnerability-disclosure-process

Cybersecurity & Infrastructure Security Agency, “Fact Sheet: TrickBot Malware,” March 2021a. As of October 2020: https://www.cisa.gov/uscert/sites/default/files/publications/TrickBot_Fact_Sheet_508.pdf

Cybersecurity & Infrastructure Security Agency, “CISA Announces New Vulnerability Disclosure Policy (VDP) Platform,” July 2021a. As of December 2021: https://www.cisa.gov/blog/2021/07/29/cisa-announces-new-vulnerability-disclosure-policy-vdp-platform

Cyber Security Agency of Singapore, *Singapore’s Cybersecurity Strategy*, Government of Singapore, 2016. As of October 2020: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

Daniel, Michael, “Heartbleed: Understanding When We Disclose Cyber Vulnerabilities,” *The White House Blog*, April 28, 2014. As of December 2020: https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

De Fina, Anna, & Alexandra Georgakopoulou, “Introduction: Narrative analysis in the shift from texts to practices,” *Text & Talk*, Vol. 28, No. 3, 2008, pp. 275-281. As of December 2021: https://doi.org/10.1515/TEXT.2008.013

Denzin, N. K. & Y. S. Lincoln, “Introduction: entering the field of qualitative research,” in: *Handbook of Qualitative Research*, 1994, pp. 1–17. SAGE Publications.

Department of Homeland Security, “The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research,” Science & Technology Directorate, 2012.

DeSombre, Winnona, James Shires, JD Work, Robert Morgus, Patrick Howell O'Neill, Luca Allodi, & Trey Herr, *Countering cyber proliferation: Zeroing in on Access-as-a-Service*, Atlantic Council, March 1, 2021. As of December 2021: https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/

Digital Transformation Team, "Digital innovation for citizens and for the development of the country," Government of Italy, n.d. As of October 2020: https://teamdigitale.governo.it/en/

Dixon, Denelle, "Improving Government Disclosure of Security Vulnerabilities," *Open Policy & Advocacy*, Mozilla, September 2016. As of October 2020: https://blog.mozilla.org/netpolicy/2016/09/19/improving-government-disclosure-of-security-vulnerabilities/

Dixon, Denelle, "Improving Internet Security through Vulnerability Disclosure," *Distilled*, Mozilla, May 2017a. As of October 2020: https://blog.mozilla.org/en/mozilla/improving-internet-security-vulnerability-disclosure/

Dixon, Denelle, "WannaCry is a Cry for VEP Reform," *Distilled*, Mozilla, May 2017b. As of October 2020: https://blog.mozilla.org/en/security/wannacry-cry-vep-reform/

Dorrestijn, Steven, & Peter-Paul Verbeek, "Technology, wellbeing, and freedom: The legacy of utopian design," *International Journal of Design*, Vol. 7, No. 3, 2013, pp. 45-56. As of October 2021: https://memphis-milano.com/wp-content/uploads/2020/01/201312InternationalMagOfDesign.pdf

Downes, Larry, "U.S. Digital Infrastructure Needs More Private Investment," Harvard Business Review, October 14, 2016. As of December 2021: https://hbr.org/2016/10/u-s-digital-infrastructure-needs-more-private-investment

Driver, Julia, "The History of Utilitarianism," *Stanford Encyclopedia of Philosophy*, 2014. As of October 2021: https://plato.stanford.edu/entries/utilitarianism-history/

Dutton, J. E., M. C. Worline, P.J. Frost, & J. Lilius, "Explaining compassion organizing," *Administrative Science Quarterly*, Vol. 51, 2006, pp. 59-96.

Eatough, Virginia, & Jonathan A. Smith, "Interpretative Phenomenological Analysis," in Carla Willig, Wendy Stainton Rogers (Eds.), *The SAGE Handbook of Qualitative Research in Psychology*, 2017.

Edwards, W. Joseph, "Attorneys Get Child Porn Charges Dropped as FBI 'Browses' into New Privacy Territory," August 2019. As of October 2020: https://www.columbusdefenselawyer.attorney/attorneys-get-fbi-charges-dropped/

Electronic Frontier Foundation v. National Security Agency, Office of the Director of National Intelligence, Case No.: 14-cv-03010-RS, February 18, 2016. As of October 2020: https://www.eff.org/document/vep-foia-effs-xmsj-and-opp

Electronic Privacy Information Center, "EPIC v. NSA: NSPD-54 Appeal," n.d.a. As of October 2020: https://epic.org/foia/nsa/nspd-54/appeal/

Electronic Privacy Information Center, "Vulnerabilities Equities Process," n.d.b. As of October 2020: https://archive.epic.org/privacy/cybersecurity/vep/

Ethics, Merriam-Webster, 2022. As of December 2020: https://www.merriam-webster.com/dictionary/ethics

European Institute of Romania, *Current Challenges In The Field Of Cybersecurity – The Impact And Romania's Contribution To The Field*, Government of Romania, 2018. As of October 2020: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf

Farivar, Cyrus, "New leak shows feds can access user accounts for Google, Facebook and more," *ARS Technica*, June 2013. As of December 2020: https://arstechnica.com/tech-policy/2013/06/new-leak-feds-can-access-anything-in-your-google-facebook-and-more/

Federal Bureau of Investigation, "Director Comey Remarks During May 11 'Pen and Pad' Briefing with Reporters [press release]," May 14, 2016. As of November 2020: https://www.fbi.gov/news/pressrel/press-releases/director-comey-remarks-during-may-11-2018pen-and-pad2019-briefing-with-reporters

Federal Bureau of Investigation, "'Playpen' Creator Sentenced to 30 Years Dark Web 'Hidden Service' Case Spawned Hundreds of Child Porn Investigations," May 5, 2017. As of November 2020: https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years

Feng, Yunfei, Carl K. Chang, & Hua Ming, "Engaging Mobile Data to Improve Human Well-being: the ADL Recognition Approach," *IT Professional IS*, 2018. As of October 2021: https://www.researchgate.net/profile/Yunfei-Feng-2/publication/317631759_Engaging_Mobile_Data_to_Improve_Human_Well-being_the_ADL_Recognition_Approach/links/5b4589cb0f7e9b1c72235889/Engaging-Mobile-Data-to-Improve-Human-Well-being-the-ADL-Recognition-Approach.pdf

Fidler, Mailyn, & Trey Herr, "PATCH: Debating Codification of the VEP," *Lawfare*, May 17, 2017. As of March 2021: https://www.lawfareblog.com/patch-debating-codification-vep

Firestone, William A., "Meaning in Method: The Rhetoric of Quantitative and Qualitative Research," *American Educational Research Association*, Vol. 16, No. 7, October 1987, pp. 16-21. As of December 2021: https://journals.sagepub.com/doi/abs/10.3102/0013189X016007016

Floridi, Luciano, “Distributed Morality in an Information Society,” *Sci Eng Ethics*, Vol. 19, 2013, pp. 727-743. doi: 10.1007/s11948-012-9413-4.

Floridi, Luciano, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Springer, 2014a.

Floridi, Luciano, *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Springer, 2014b. As of October 2021: https://library.oapen.org/bitstream/handle/20.500.12657/28025/1001971.pdf?sequence=1#page=90

Floridi, Luciano, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, Christoph Luetge, Robert Madelin, Ugo Pagallo, Francesca Rossi, Burkhard Schafer, Peggy Valcke, & Effy Vayena, “AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations,” *Minds and Machines*, Vol. 28, 2018, pp. 689–707. As of October 2021: https://link.springer.com/article/10.1007/s11023-018-9482-5

Floridi, Luciano, Josh Cowls1, Thomas C. King, & Mariarosaria Taddeo, “How to Design AI for Social Good: Seven Essential Factors,” *Science and Engineering Ethics*, Vol. 26, 2020, pp. 1771–1796. As of October 2021: https://doi.org/10.1007/s11948-020-00213-5

Formosa, Paul, Michael Wilson, & Deborah Richards, “A Principlist Framework for Cybersecurity Ethics,” *Computers & Security*, Vol. 109, 2021. As of October 2021: https://doi.org/10.1016/j.cose.2021.102382

Francis, JJ., M. Johnston, C. Robertson, L. Glidewell, V. Entwistle, MP. Eccles, et al., “What is an adequate sample size? Operationalising data saturation for theory-based interview studies,” *Psychology & Health*, Vol. 25, No. 10, 2010, pp. 1229-1245.

Fung, Brian, “Microsoft takes down massive hacking operation that could have affected the election,” *CNN* Business, October 2020. As of November 2020: https://www.cnn.com/2020/10/12/tech/microsoft-election-ransomware/index.html?form=MY01SV&OCID=MY01SV

Gallagher, Sean, “The Snowden Legacy, part one: What’s changed, really?,” *ARS Technica*, November 2018. As of December 2020: https://arstechnica.com/tech-policy/2018/11/the-snowden-legacy-part-one-whats-changed-really/

Garcia-Ceja, Enrique, Venet Osmani, & Oscar Mayora, “Automatic Stress Detection in Working Environments From Smartphones’ Accelerometer Data: A First Step," *IEEE Journal of Biomedical and Health Informatics*, Vol. 20, No. 4, 2016, pp. 1053-1060. doi: 10.1109/JBHI.2015.2446195.

Garlington, Sarah B., Mary Elizabeth Collins, & Margaret R. Durham Bossaller, "An Ethical Foundation for Social Good: Virtue Theory and Solidarity," *Research on Social Work Practice*, Vol. 30, No. 2, 2020, pp. 196-204. As of October 2021: https://doi.org/10.1177/1049731519863487

Gates, Megan, "The Zero Day Problem," *Security Management*, November 1, 2017. As of November 2020: https://www.asisonline.org/security-management-magazine/articles/2017/11/the-zero-day-problem/

Gay, L. R., & P. Airasian, (2000) *Educational Research: competencies for analysis and application* (6th edition). Pearson Higher Ed.

Geiger, A.W., "How Americans have viewed government surveillance and privacy since Snowden leaks," *Pew Research Center*, June 2018. As of October 2020: https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/

Gelo, O., D. Braakmann, & G. Benetka, "Quantitative and Qualitative Research: Beyond the Debate." *Integrative Psychological and Behavioral Science*, Vol. 42, 2008, pp. 266–290. https://doi.org/10.1007/s12124-008-9078-3

Gillmor, Daniel Kahn, & Leigh Honeywell, "US Government Malware Policy Puts Everyone At Risk," American Civil Liberties Union, June 2017. As of October 2020: https://www.aclu.org/blog/privacy-technology/internet-privacy/us-government-malware-policy-puts-everyone-risk

Global Forum on Cyber Expertise, n.d. As of October 2020: https://thegfce.org/

Government of Canada, *CSE's Equities Management Framework*, 2019. As of November 2020: https://cse-cst.gc.ca/en/information-and-resources/announcements/cses-equities-management-framework

Government Communications Headquarters, "The Equities Process," Government of the United Kingdom, November 2018. As of October 2020: https://www.gchq.gov.uk/information/equities-process

Government Technology Agency, "Vulnerability Disclosure Programme," Government of Singapore, n.d. As of October 2020: https://www.tech.gov.sg/report_vulnerability

Greene, Jay, & Ellen Nakashima, "Microsoft seeks to disrupt Russian criminal botnet it fears could seek to sow confusion in the presidential election," *The Washington Post*, October 2020. As of November 2020: https://www.washingtonpost.com/technology/2020/10/12/microsoft-trickbot-ransomware/

Greenwald, Glenn, “NSA collecting phone records of millions of Verizon customers daily,” *The Guardian*, June 6, 2013. As of October 2020: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, Glenn, & Ewen MacAskill, “Boundless Informant: the NSA's secret tool to track global surveillance data,” *The Guardian*, June 11, 2013. As of October 2020: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

Guest, Greg, E. Namey, M. Chen, “A simple method to assess and report thematic saturation in qualitative research,” *Public Health Implications of a Changing Climate*, 2020. As of December 2021: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0232076

Guest, Greg, Kathleen M. MacQueen, & Emily E. Namey, “Introduction to Applied Thematic Analysis,” in *Applied Thematic Analysis*, SAGE Research Methods, 2014. As of December 2021: http://antle.iat.sfu.ca/wp-content/uploads/Guest_2012_AppliedThematicAnlaysis_Ch1.pdf

Guest, Greg, A. Bunce, & L. Johnson, “How many interviews are enough? an experiment with data saturation and variability,” *Field Methods*, Vol. 18, 2006, pp. 59-82.

Hagaman, A., & K. Wutich, “How many interviews are enough to identify metathemes in multisited and cross-cultural research? Another perspective on Guest, Bunce, and Johnson's (2006) landmark study,” *Field Methods,* Vol. 29, 2017, pp. 23-41.

Haracic, Armin, "White House calls for greater transparency in cyber Vulnerability Equities Process," *Fifth Domain*, November 15, 2017. As of October 2020: https://www.fifthdomain.com/civilian/2017/11/15/white-house-calls-for-greater-transparency-in-cyber-vulnerabilities-equities-process/

Harcourt, Bernard E., “The collapse of the harm principle,” *J. Crim. Law Criminol.*, Vol. 90, No. 1, 1999, pp. 109-194. As of October 2021: https://heinonline.org/HOL/Page?handle=hein.journals/jclc90&div=10&g_sent=1&casa_token=&collection=journals

Heckman, Jory, "Hackers not yet pulling out big guns for data breaches, NSA official warns," Federal News Network, October 18, 2016. As of November 2020: https://federalnewsnetwork.com/technology-main/2016/10/hackers-not-yet-pulling-big-guns-data-breaches-nsa-official-warns/

Healey, Jason, “The US Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers,” *Journal of International Affairs*, November 2016. As of Oct 2020: https://jia.sipa.columbia.edu/sites/default/files/attachments/Healey%20VEP.pdf

Heller, Michael, “Federal vulnerability review under new VEP still has questions,” *TechTarget*, November 2017. As of December 2021:

https://www.techtarget.com/searchsecurity/news/450430245/Federal-vulnerability-review-under-new-VEP-still-has-questions

Herman, Michael, *Intelligence Power In Peace and War*, Royal Institute of International Affairs, Cambridge University, 1996. As of December 2021: https://people.exeter.ac.uk/mm394/Michael%20Herman%20Intelligence%20Power%20in%20Peace%20and%20War%20%201996.pdf

Herpig, Sven, "Governmental Vulnerability Assessment and Management: Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities," *Stiftung Neue Verantwortung*, August 2018. As of November 2020: https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf

Herpig, Sven & Ari Schwartz, "The Future of Vulnerabilities Equities Processes Around the World," *Lawfare*, January 4, 2019. As of October 2020: https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world

Hesseldahl Arik, "Snowden Leaks Have Changed How Americans See Their Privacy," *Vox*, As of October 2020: https://www.vox.com/2015/3/16/11560290/snowden-leaks-have-changed-how-americans-see-their-privacy

Hildebrandt, Mireille, "Balance or Trade-off ? Online Security Technologies and Fundamental Rights," *Philos. Technol.*, Vol. 26, No. 4, 2013, pp. 357-379. As of October 2021: https://link.springer.com/article/10.1007%2Fs13347-013-0104-0

Hooker, R. S., "Do physician assistants provide a "social good" for America?," *Journal of the American Academy of Physician Assistants*, Vol. 22, No. 12, 2009.

Hosenball, Mark, & Will Dunham, "White House, spy agencies deny NSA exploited 'Heartbleed' bug," *Reuters*, April 11, 2014. As of December 2020: https://www.reuters.com/article/instant-article/idUKBREA3A1XD20140411

İbrahimoğlu, Nurettin, Şemsettin Çiğdem, Mehmet Seyhan, "Relationship between culture & ethic: a research in terms of cultural diversity," Procedia - Social and Behavioral Sciences, Vol. 143, 2014, pp. 1117-1119.

Ijsselsteijn, Wijnand, Yvonne de Kort, Cees Midden, Berry Eggen, & Elise van den Hoven, "Persuasive Technology for Human Well-Being: Setting the Scene," *Computer Science*, Vol. 3962, 2006. As of October 2021: https://doi.org/10.1007/11755494_1

Informācijas technoloģiju drošības incidentu novēršanas institūcijas, "CERT.LV Responsible disclosure policy," Government of Latvia, September 2016. As of October 2020: https://www.cert.lv/en/about-us/responsible-disclosure-policy

Information-technology Promotion Agency, “About Information Security Early Warning Partnership,” Japanese Ministry of Economy, Trade and Industry, n.d.a. As of October 2020: https://www.ipa.go.jp/security/english/about_partnership.html

Information-technology Promotion Agency, “Information Security Early Warning Partnership: Overview of Vulnerability Handling Process,” Japanese Ministry of Economy, Trade and Industry, n.d.b. As of October 2020: https://www.ipa.go.jp/files/000044732.pdf

Johnson, James T., “Just War: International Law,” *Britannica*, n.d. As of December 2021: https://www.britannica.com/topic/just-war

JPCERTCC, “Security Alerts,” n.d.a. As of December 2021: https://www.jpcert.or.jp/english/at/2021.html

JPCERTCC, “Japan Vulnerability Notes,” n.d.b. As of December 2021: https://jvn.jp/en/

Katagiri, Nori, “Why international law and norms do little in preventing non-state cyber attacks,” *Journal of Cybersecurity*, Vol. 7, No. 1, 2021. As of December 2021: https://academic.oup.com/cybersecurity/article/7/1/tyab009/6168044

Kelley, Michael B., “The US Now Thinks Snowden 'Probably Downloaded' 1.5 Million Documents That Haven't Been Found,” *Insider*, June 2014. As of October 2020: https://www.businessinsider.com/clapper-says-snowden-took-less-than-they-though-2014-6

King, N., “Using templates in the thematic analysis of text,” in Cassell, C., Symon, G. (Eds.), *Essential guide to qualitative methods in organizational research*, 2004, pp. 257-270. London, UK: Sage.

Kirk, Jeremy, “Mozilla Presses Government to Reveal Firefox Vulnerability,” *Bank Info Security*, May 2016. As of October 2020: https://www.bankinfosecurity.com/mozilla-presses-government-to-reveal-firefox-vulnerability-a-9102

Klein, Adam, Michèle Flournoy, & Richard Fontaine, “Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond,” *Center for a New American Security*, December 2016. As of November 2020: https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Surveillance-Final.pdf

Knake, Robert, "Grading the New Vulnerabilities Equities Policy: Pass," *Council on Foreign Relations*, November 16, 2017. As of November 2020: https://www.cfr.org/blog/grading-new-vulnerabilities-equities-policy-pass

Krebs, Brian, “Firefox Zero-Day Used in Child Porn Hunt?,” *Krebs on Security*, August 2013. As of November 2020: https://krebsonsecurity.com/2013/08/firefox-zero-day-used-in-child-porn-hunt/

Krippendorff, Klaus, *Content Analysis: An Introduction to Its Methodology*, 2018. SAGE Publications

Lawfare, *Snowden Revelations*, n.d. As of December 2020: https://www.lawfareblog.com/snowden-revelations

Lee, Timothy B., "The Heartbleed Bug, Explained," *Vox*, May 2015. As of December 2020: https://www.vox.com/2014/6/19/18076318/heartbleed

Lee, Seung, "FBI Doesn't Have to Give Mozilla Details on Bug It Used to Bust a Child Porn Ring," May 2016. As of October 2020: https://www.newsweek.com/fbi-doesnt-have-give-mozilla-details-bug-it-used-bust-child-porn-ring-461325

Lejano, R. P., *Frameworks for policy analysis: Merging text & Context*, New York, NY: Routledge, 2006.

Levy, Ian, "Equities Process," National Cyber Security Centre, November 2018. As of October 2020: https://www.ncsc.gov.uk/blog-post/equities-process

Lincoln, Yvonne S., & Egon G. Guba, *Naturalistic Inquiry*, 1985. Newbury Park, CA: SAGE Publications.

Loi, Michele, & Markus Christen, "Ethical frameworks for cybersecurity," *The Ethics of Cybersecurity*, Springer, 2020, pp. 73-96. As of October 2021: https://library.oapen.org/bitstream/handle/20.500.12657/47324/9783030290535.pdf?sequence=1#page=88

Lyngaas, Sean, "NSA says it found new critical vulnerabilities in Microsoft Exchange Server," *CyberScoop*, April 2021. As of May 2021: https://www.cyberscoop.com/nsa-microsoft-exchange-server-vulnerabilities/

Markendahl, Jan, Stefan Lundberg, Olga Kordas, & Staffan Movin, "On the role and potential of IoT in different industries: Analysis of actor cooperation and challenges for introduction of new technology," *Internet of Things Business Models, Users, and Networks*, 2017, pp. 1-8. doi: 10.1109/CTTE.2017.8260988.

Martinez, Cindy, "Flaws in the U.S. Vulnerabilities Equities Process," OODALoop, January 2020. As of October 2020: https://www.oodaloop.com/archive/2020/01/24/flaws-in-the-u-s-vulnerabilities-equities-process/

McBeath, B., "Re-envisioning macro social work practice," *Families in Society: The Journal of Contemporary Social Services*, Vol. 97, No. 1, 2016, pp. 5-14.

McElwee, Brian, "The rights and wrongs of consequentialism," *Philosophical Studies*, Vol 151, 2010, pp. 393-412. As of October 2021: https://link.springer.com/article/10.1007/s11098-009-9458-7

Microsoft, "Microsoft takes action to disrupt botnet and combat ransomware," October 2020. As of November 2020: https://news.microsoft.com/apac/2020/10/13/microsoft-takes-action-to-disrupt-botnet-and-combat-ransomware/

Microsoft, "Partnering with governments to help protect democracy," n.d. As of December 2021: https://www.microsoft.com/en-us/security/business/government

Ministry Of National Defence Republic Of Lithuania, "Lithuania starts work to create legal framework for ethical hackers," Government of Lithuania, September 2020. As of October 2020: http://kam.lt/en/news_1098/current_issues/lithuania_starts_work_to_create_legal_framework_for_ethical_hackers.html

Mittelstadt, Brent, "Ethics of the health-related internet of things: a narrative review," *Ethics Inf Technol*, Vol. 19, 2017, pp. 157-175. As of October 2021: https://doi.org/10.1007/s10676-017-9426-4

Mor Barak, M. E., "The practice & science of social good: Emerging paths to positive social impact," *Research on Social Work Practice*, 2018, pp. 1-12. doi:10.1177/1049731517745600

Morgan, Gwenyth & Bert Gordijn, "A care-based stakeholder approach to ethics of cybersecurity in business," *The Ethics of Cybersecurity*, Springer, 2020, pp. 119-138. As of October 2021: https://library.oapen.org/bitstream/handle/20.500.12657/22489/1007696.pdf?sequence=1#page=131

Morgan, M., B. Fischoff, A. Bostrom, & C. Atman, *Risk Communication: A Mental Models Approach,* New York, NY: Cambridge University Press; 2002.

Mozilla, "Mozilla Foundation forms new organization to further the creation of free, open source internet software, including the award-winning Mozilla Firefox browser," August 2005. As of December 2021: https://blog.mozilla.org/press/2005/08/mozilla-foundation-forms-new-organization-to-further-the-creation-of-free-open-source-internet-software-including-the-award-winning-mozilla-firefox-browser/

Mozilla, "Investigating Security Vulnerability Report," August 2013. As of October 2020: https://blog.mozilla.org/security/2013/08/04/investigating-security-vulnerability-report/

Mozilla, "The Vulnerabilities Equities Process: What we know and what we'd like to see," 2017. As of October 2020: https://blog.mozilla.org/press/files/2017/05/VEP-WhatWeKnow.pdf

Mozilla, "The Mozilla Manifesto Addendum Pledge for a Healthy Internet," n.d. As of December 2021: https://www.mozilla.org/en-US/about/manifesto/

Mukerji, Nikil, "The Case Against Consequentialism: Methodological Issues," In Miguel Holtje, Thomas Spitzley & Wolfgang Spohn (eds.), *GAP.8 Proceedings, Gesellschaft für*

Analytische Philosophie, 2013, pp. 654-665. As of October 2021: https://philpapers.org/rec/MUKTCA

Namey, E., G. Guest, K. McKenna, & M. Chen, "Evaluating Bang for the Buck: A Cost-Effectiveness Comparison Between Individual Interviews and Focus Groups Based on Thematic Saturation Levels," *American Journal of Evaluation*, Vol. 37, No. 3, 2016, pp. 425-40.

National Cyber Security Centre, "Coordinated Vulnerability Disclosure: the Guideline," Ministry of Justice and Security, Government of the United Kingdom, November 2018a. As of October 2020: https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline

National Cyber Security Centre, "GCHQ and the NCSC publish the UK Equities Process," Ministry of Justice and Security, Government of the United Kingdom, November 2018b. As of October 2020: https://www.ncsc.gov.uk/news/gchq-and-ncsc-publish-uk-equities-process

Newman, Lily Hay, " The Feds Would Rather Drop a Child Porn Case Than Give Up a Tor Exploit," *Wired*, March 2017a. As of October 2020: https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/

Newman, Lily Hay, "Feds Explain Their Software Bug Stash – But Don't Erase Concerns," *Wired*, November 2017b. As of October 2020: https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/

Nowell, Lorelli S., Jill M. Norris, Deborah E. White, & Nancy J. Moules, Thematic Analysis: Striving to Meet the Trustworthiness Criteria," *International Journal of Qualitative Methods*, Vol. 16, No. 1, October 2017. As of December 2021: https://doi.org/10.1177/1609406917733847

Office of the Director of National Intelligence, "Statement on Bloomberg News story that NSA knew about the "Heartbleed bug" flaw and regularly used it to gather critical intelligence," April 11, 2014. As of December 2020: https://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew

Office of the Director of National Intelligence, "Members of the IC," n.d. As of December 2020: https://www.dni.gov/index.php/what-we-do/members-of-the-ic

O'Neil, Michael, "Cybercrime Dilemma: Is it Possible to Guarantee Both Security and Privacy?," *Brookings*, 2001. As of December 2021: https://www.brookings.edu/articles/cybercrime-dilemma-is-it-possible-to-guarantee-both-security-and-privacy/

Overeem, P., & B. Tholen, “After managerialism: MacIntyre’s lessons for the study of public administration,” *Administration and Society*, Vol. 43, 2011, pp. 722-748.

Patrick, Colin, “Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations,” *Washington International Law Journal*, Vol. 28, No. 2, 2019, pp. 581-604. As of December 2021: https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1811&context=wilj

Pedreshi, Dino, Salvatore Ruggieri, & Franco Turini, *Discrimination-aware data mining, Conference Proceedings*, Las Vegas: 14th ACM SIGKDD international conference on Knowledge discovery and data mining, 2008. As of October 2021: https://doi.org/10.1145/1401890.1401959

Pell, Stephanie K., & LTC James Finocchiaro, “The Ethical Imperative for a Vulnerability Equities Process and How the Common Vulnerability Scoring System Can Aid that Process,” *Connecticut Law Review*, Vol. 49, No. 5, 2017, pp. 1551-1589.

Perlroth, Nicole, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*, 2021. Bloomsbury Publishing.

Peterson, Andrea, "Why everyone is left less secure when the NSA doesn't help fix security flaws," *The Washington Post*, October 4, 2013. As of November 2020: https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws/?utm_term=.d9144ccc8071

Pupillo, Lorenzo, "Software Vulnerabilities Disclosure: The European landscape," Centre for European Policy Studies, July 31, 2017. As of November 2020: https://www.ceps.eu/ceps-publications/software-vulnerabilities-disclosure-european-landscape/

Riley, Michael, “NSA Said to Have Used Heartbleed Bug, Exposing Consumers,” *Bloomberg*, April 11, 2014. As of December 2020: https://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers

Roeser, Sabine, “Emotional Engineers: Toward Morally Responsible Design,” *Sci Eng Ethics*, Vol. 18, 2012, pp. 103-115. As of October 2021: https://doi.org/10.1007/s11948-010-9236-0

Rumold, Mark, “Playpen: The Story of the FBI’s Unprecedented and Illegal Hacking Operation,” Electronic Frontier Foundation, September 2016. As of October 2020: https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation

Saldana, Johnny, *The Coding Manual for Qualitative Researchers*, Third Edition, 2015. SAGE Publications.

Sanchez, Julian, The NSA's Heartbleed Problem Is the Problem with the NSA," *CATO Institute*, April 12, 2014. As of December 2020: https://www.cato.org/publications/commentary/nsas-heartbleed-problem-problem-nsa

Sanger, David E., & Nicole Perlroth, "Microsoft Takes Down a Risk to the Election, and Finds the U.S. Doing the Same," October 2020. As of October 2020: https://www.nytimes.com/2020/10/12/us/politics/election-hacking-microsoft.html

Sasso, Brendan, "Google Knew About Heartbleed and Didn't Tell the Government," *The Atlantic*, April 14, 2014. As of December 2020: https://www.theatlantic.com/politics/archive/2014/04/google-knew-about-heartbleed-and-didnt-tell-the-government/457071/

Schaake, Marietje, Lorenzo Pupillo, Afonso Ferreira, & Gianluca Varisco, eds., *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges*, CEPS Task Force, June 2018. As of October 2020: https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf

Schneier, Bruce, "New leaks prove it: the NSA is putting us all at risk to be hacked," *Vox*, Aug 24, 2016. As of November 2020: https://www.vox.com/2016/8/24/12615258/nsa-security-breach-hoard

Schwartz, Ari, & Robert Knake, "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process," Cyber Security Project, Belfer Center, June 2016. As of November 2020: https://www.belfercenter.org/publication/governments-role-vulnerability-disclosure-creating-permanent-and-accountable

Senate Committee on Armed Services, *Hearing to Receive Testimony on Encryption and Cyber Matters*, September 13, 2016. As of November 2020: https://www.armed-services.senate.gov/imo/media/doc/16-68_09-13-16.pdf

Shukla, Rajesh C., "Public Policy and Social Good: Theory, Practice and Beyond," *Ethics in Economic Life*, Vol. 20, No. 4, 2017, pp. 19-35. doi: http://dx.doi.org/10.18778/1899-2226.20.4.02

Simone, Maria A., "Give me liberty and give me surveillance," *Crit. Discourse Stud.*, Vol. 6, No. 1, 2009, pp. 1-14. As of October 2021: https://doi.org/10.1080/17405900802559977

Sinche, Soraya, Ricardo Barbosa, David Nunes, Ashley Figueira, & Jorge Sá Silva, "Wireless sensors and mobile phones for human well-being," *2017 IEEE XXIV International Conference on Electronics*, *Electrical Engineering and Computing (INTERCON)*, 2017, pp. 1-4. doi: 10.1109/INTERCON.2017.8079641.

Sinnott-Armstrong, Walter, “Consequentialism,” *Stanford Encyclopedia of Philosophy*, 2019. As of October 2021: https://plato.stanford.edu/entries/consequentialism/?utm_campaign=Matt%27s%20Thoughts%20In%20Between&utm_medium=email&utm_source=Revue%20newsletter

Smith, Brad, "The need for a Digital Geneva Convention," Microsoft, February 14, 2017a. As of November 2020: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001gnysbhjsod01z7q11hvz0xg2d

Smith, Brad, "The need for urgent collective action to keep people safe online: Lessons from last week’s cyberattack," Microsoft, May 14, 2017b. As of November 2020: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Smith, Bryant Walker, “The Trolley and the Pinto: Cost-Benefit Analysis in Automated Driving and Other Cyber-Physical Systems,” *Texas A&M Law Review*, Vol. 4, 2017c, pp. 197-208. As of October 2021: https://scholarship.law.tamu.edu/lawreview/vol4/iss2/5/

Stisa Granick, Jennifer, “Trump’s New Cybersecurity Rules Are Better Than Obama’s,” American Civil Liberties Union, November 2017. As of December 2021: https://www.aclu.org/blog/privacy-technology/internet-privacy/trumps-new-cybersecurity-rules-are-better-obamas

Synopsis, *The Heartbleed Bug*, March 2020. As of December 2020: https://heartbleed.com/

Szostak, R., “Politics and the five types of ethical analysis,” *International Journal of Politics and Ethics*, Vol. 2, 2002, pp. 275-290.

Szostak, R., *Unifying Ethics*. Lanham, MD: University Press of America, 2005.

Tech Accord, "Governments need to do more, and say more, on vulnerability handling," September 10, 2018. As of November 2020: https://cybertechaccord.org/government-vulnerability-handling/

Ter Meulen, R., “Solidarity, justice, & recognition of the other,” *Theoretical Medicine and Bioethics*, Vol. 37, 2016, pp. 517-529.

Terry, Gareth, Nikki Hayfield, Victoria Clarke, & Virginia Braun, “Thematic Analysis,” in *The SAGE Handbook of Qualitative Research in Psychology*, SAGE Publications, 2017.

TrendMicro, “Botnet,” n.d. As of December 2021: https://www.trendmicro.com/vinfo/us/security/definition/botnet

U.S. Senate Committee on Homeland Security & Governmental Affairs, “Majority Media: Lieberman and Collins step up scrutiny of cyber security initiative,” May 2, 2008. As of

December 2020: https://www.hsgac.senate.gov/media/majority-media/lieberman-and-collins-step-up-scrutiny-of-cyber-security-initiative

Vaismoradi, Mojtaba, Jacqueline Jones, Hannele Turunen, & Sherrill Snelgrove, "Theme development in qualitative content analysis and thematic analysis," *Journal of Nursing Education and Practice*, Vol. 6, No. 5, pp. 100-110. DOI: 10.5430/jnep.v6n5p100

Vallor, Shannon, *An Introduction to Cybersecurity Ethics*, Markkula Center for Applied Ethics (Santa Clara University), 2018. As of October 2021: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf

Vallor, Shannon, *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*, Oxford University Press: 2016.

Van de Poel, Ibo, "Core values and value conflicts in cybersecurity," *The Ethics of Cybersecurity*, Springer, 2020, pp. 45-72. As of October 2021: https://library.oapen.org/bitstream/handle/20.500.12657/47324/9783030290535.pdf?sequence=1#page=61

Van Dijk, Teun A., "Ideology and discourse analysis," *Journal of Political Ideologies*, Vol. 11, No. 2, 2007, pp. 115-140. https://doi.org/10.1080/13569310600687908

Verdugo, R. R., "School reform: Community, corporatism, & the social good," *International Journal of Educational Reform*, Vol. 22, No. 118, 2013.

Vijayan, Jai, "White House Releases New Charter for Using, Disclosing Security Vulnerabilities," *DARKReading*, November 15, 2017. As of October 2020: https://www.darkreading.com/attacks-breaches/white-house-releases-new-charter-for-using-disclosing-security-vulnerabilities-/d/d-id/1330445

Ward, Vicky, Allan House, & Susan Hamer, "Developing a Framework for Transferring Knowledge Into Action: A Thematic Analysis of the Literature," Journal of Health Services Research & Policy, Vol. 14, No. 3, 2017, pp. 156-164. As of December 2021: https://journals.sagepub.com/doi/full/10.1258/jhsrp.2009.008120

Weaver, G. R., "Virtue in organizations: Moral identity as a foundation for moral agency," *Organization Studies*, 27, 2006, pp. 341-368.

Weber, Karsten, & Nadine Kleine, "Cybersecurity in health care," *The Ethics of Cybersecurity*, Springer, 2020, pp. 139-156. As of October 2021: https://library.oapen.org/bitstream/handle/20.500.12657/47324/9783030290535.pdf?sequence=1#page=151

West, Heather, "Mozilla Asks President Obama to Help Strengthen Cybersecurity," *Open Policy & Advocacy*, Mozilla, October 2016. As of October 2020:

https://blog.mozilla.org/netpolicy/2016/10/25/mozilla-asks-president-obama-to-help-strengthen-cybersecurity/

West, Heather, “Working Together Towards a more Secure Internet through VEP Reform,” *Open Policy & Advocacy*, Mozilla, May 2017a. As of October 2020: https://blog.mozilla.org/netpolicy/2017/05/17/working-together-towards-secure-internet-vep-reform/

West, Heather, “White House releases new VEP charter,” *Open Policy & Advocacy*, Mozilla, November 2017b. As of October 2020: https://blog.mozilla.org/netpolicy/2017/11/15/white-house-releases-new-vep-charter/

White House, "Memorandum for Recipients of NSPD-54/HSPD-23," January 9, 2008. As of October 2020: https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf

White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009. As of December 2020: https://nsarchive.gwu.edu/document/21424-document-28

White House, *The Comprehensive National Cybersecurity Initiative*, 2010. As of December 2020: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf

White House, *National Security Presidential Memorandum-4: Organization of the National Security Council, the Homeland Security Council, and Subcommittees*, April 4, 2017a. As of December 2020: https://www.whitehouse.gov/presidential-actions/national-security-presidential-memorandum-4/

White House, *Vulnerabilities Equities Policy and Process for the United States Government*, November 15, 2017b. As of December 2020: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

Whittaker, Zack, “How the NSA shot itself in the foot by denying prior knowledge of Heartbleed vulnerability,” *ZDNet*, April 12, 2014. As of December 2020: https://www.zdnet.com/article/how-the-nsa-shot-itself-in-the-foot-by-denying-prior-knowledge-of-heartbleed-vulnerability/

Wilson, Andi, Ross Schulman, Kevin Bankston, & Trey Herr, *Bugs in the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications*, July 2016. As of November 2020: https://na-production.s3.amazonaws.com/documents/Bugs-in-the-System-Final.pdf

Wittes, Benjamin, “NSA Knew About and Exploited Heartbleed---Unless it Didn't,” *Lawfare*, April 11, 2014. As of December 2020: https://www.lawfareblog.com/nsa-knew-about-and-exploited-heartbleed-unless-it-didnt

Wright, Jennifer Cole, Michael T. Warren, & Nancy E. Snow, Understanding Virtue: Theory and Measurement, Oxford University Press, 2021.

Wright, T. A., & J. Goodstein, "Character is not "dead" in management research: A review of individual character & organizational-level virtue," *Journal of Management*, Vol. 33, 2007, pp. 928-958.

Yilmaz, Kaya, "Comparison of Quantitative and Qualitative Research Traditions: epistemological, theoretical, and methodological differences," *European Journal of Education Research, Development, and Policy*, Vol. 48, No. 2, June 2013, pp. 311-325. As of December 2021: https://onlinelibrary.wiley.com/doi/full/10.1111/ejed.12014

Zetter, Kim, "Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years," *Wired*, April 11, 2014. As of December 2020: https://www.wired.com/2014/04/nsa-exploited-heartbleed-two-years/

Zhang, Daniel, "Vulnerabilities Equities Process Revisited," *Georgetown Security Studies Review*, May 28, 2019. As of October 2020: https://georgetownsecuritystudiesreview.org/2019/05/28/vulnerabilities-equities-process-revisited/