Debugging the System: Reforming Vulnerability Disclosure Programs in the Private Sector

Jasmine Arooni*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School; B.A., Political Science & Entrepreneurship, The University of California, Los Angeles (UCLA). Thank you to the dedicated Federal Communications Law Journal staff for bringing this Note to publication. Special thanks to Meredith Rose, Journal Adjunct, and Atena Sheibani-Nejad, Notes Editor, for their patience and encouragement from start to finish. I would also like to express my gratitude to Professor Daniel J. Solove for his guidance during the writing process and mentorship throughout my law school career. Finally, many thanks to my family for their unconditional love and support.

I. INTRODUCTION

Virtually everything is hackable in today's interconnected world.[1] While a surge of technological advancement confers numerous benefits, it also brings an increased risk of software vulnerabilities.[2] Vulnerabilities are weaknesses in software, including online systems, that can be exploited to damage the confidentiality, integrity, or availability of those systems.[3] Vulnerabilities pose risks of aftermarket exploitation, often in the form of data breaches perpetrated by malicious actors.[4] Remediation of a data breach, on average, costs $3.92 million.[5]

A Vulnerability Disclosure Program ("VDP")[6] is an increasingly popular method to mitigate vulnerability-related risks.[7] VDPs involve enlisting "hackers" (referred to in this Note as "security researchers" for neutrality), to find vulnerabilities before weaknesses can be exploited. Security researchers, in turn, are compensated for their efforts. The cost of paying researchers through a VDP is a small fraction of what it costs to remediate a data breach, as the average VDP payout is $2,041.[8]

In an age where organizations of all shapes and sizes depend on software-based technologies, addressing vulnerabilities quickly is at the crux

1. *See* Roger A. Grimes, *Everything Is Hackable-and Cyber Criminals Can't Be Tracked*, CSO (May 10, 2011), https://www.csoonline.com/article/2621721/everything-is-hackable----and-cyber-criminals-can-t-be-tracked.html [https://perma.cc/K2NV-42D7].

2. *See* AWARENESS AND ADOPTION GRP., NAT'L TELECOMM. & INFO. ASS'N, VULNERABILITY DISCLOSURE ATTITUDES AND ACTIONS 3 (2016), https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf [https://perma.cc/MV8H-ETFX].

3. *Id.*

4. *See* ALLEN D. HOUSEHOLDER ET. AL, CARNEGIE MELLON UNIVERSITY, THE CERT GUIDE TO COORDINATED VULNERABILITY DISCLOSURE, SOFTWARE ENGINEERING INSTITUTE 2 (2017), https://resources.sei.cmu.edu/asset_files/specialreport/2017_003_001_503340.pdf [https://perma.cc/7DH4-PEYL].

5. *See* IBM SEC., COST OF A DATA BREACH REPORT 18 (2019), https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf [https://perma.cc/3YAM-D23K].

6. It is important to distinguish the difference between bug bounty programs (BBP) and vulnerability disclosure programs (VDP). A VDP is when a host organization (vendor) invites ethical white hat hacks to explore the organization's systems and report the discovered vulnerabilities to the organization. BBP is a form of VDP by which the organization provides monetary or other incentives for responsibly discovering and reporting vulnerability information. For the purposes of this Note, VDPs and BBPs are referred to collectively as VDPs.

7. *See* LUCA ALLODI & JUKKA RUOHONEN, A BUG BOUNTY PERSPECTIVE ON THE DISCLOSURE OF WEB VULNERABILITIES 1 (2018), https://arxiv.org/pdf/1805.09850.pdf [https://perma.cc/B4C6-RC65].

8. *See* Matt Honea, *Safe Harbor Programs: Ensuring the Bounty Isn't on White Hat Hackers' Heads,* DARK READING, (Apr. 10, 2019), https://www.darkreading.com/application-security/safe-harbor-programs-ensuring-the-bounty-isnt-on-white-hat-hackers-heads/a/d-id/1334339 [https://perma.cc/H4KE-AXFC].

of maintaining an effective security posture.[9] The growing popularity of VDPs indicates that crowdsourced bug discovery brings cost-effective solutions that may surpass in-house security strategies to address vulnerabilities. Organizations that run VDPs ("host organizations") delegate the probing of their internal systems to security researchers who perform testing remotely.[10] By harvesting the potential of security research through VDPs, host organizations may establish scalable solutions to cybersecurity challenges.[11] VDPs provide for around-the-clock security services due to their remote and global nature and may replace or supplement the otherwise-burdensome process of in-house vulnerability management.[12] Today, security research is a vital element of the cybersecurity industry, helping strengthen host organization systems used by billions worldwide.[13]

However, security researchers worry about the legal implications of their VDP participation given the realistic possibility that legal action may follow from conducting research outside of the technical or contractual scope allotted by a host organization.[14] Anti-hacking laws in the U.S., combined with an industry standard of poorly drafted legal terms in private sector VDPs, create a prohibitive and liability-laden environment for security researchers.[15]

Some VDPs offer rewards for vulnerabilities that require researchers to conduct research in direct violation of their legal terms, a practice that violates anti-hacking laws.[16] The search for a specific vulnerability solicited by the host organization might involve research that, under the organization's legal terms, is a violation or not clearly defined as proper or improper activity.[17] In turn, inconsistent or incomplete legal terms can subject a security researcher to the risk of prosecution under current anti-hacking laws in violation of those terms.[18] These poorly drafted terms force researchers to bear the risk. They

9. *See generally* Press Release, BugCrowd, Bugcrowd Announces Industry's First Platform-Enabled Cybersecurity Assessments for Marketplaces (Aug. 6, 2019), https://www.bugcrowd.com/press-release/bugcrowd-announces-industrys-first-platform-enabled-cybersecurity-assessments-for-marketplaces/ [https://perma.cc/3HZ5-CV5H].

10. *Id.*

11. *See* David A. Newman, *Bug-Bounty Programs: A Valuable Tool to Be Used Carefully*, MORRISON FOERSTER (Feb. 18, 2018), https://www.mofo.com/resources/insights/180220-bug-bounty-programs.html [https://perma.cc/Z7EG-9NEU].

12. *See* ALLODI & RUOHONEN, *supra* note 7, at 3.

13. *See The Importance of Security Research: Four Case Studies*, CTR. FOR DEMOCRACY & TECH. (Dec. 2017), https://cdt.org/files/2017/12/2017-12-15-Importance-of-Security-Research.pdf [https://perma.cc/KNC5-VRND].

14. *See* Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. Rev. 383, 397 (2014) (explaining that not all hacking is created equal, as nearly all hacking under bug bounty programs may be illegal if a program's contractual language is not properly crafted).

15. *See* J.M. Porup, *Do You Need A Vulnerability Disclosure Program? The Feds Say Yes*, CSO (Aug. 7, 2018), https://www.csoonline.com/article/3294418/do-you-need-a-vulnerability-disclosure-program-the-feds-say-yes.html [https://perma.cc/P9HS-EH92].

16. *See generally id.*

17. *Id.*

18. *Id.*

must decide their willingness to participate in a program that may not protect them from liability should their research be construed as improper.[19]

To this end, the U.S. federal government has made numerous guiding efforts, one of them being the Department of Justice's "Framework for a Vulnerability Disclosure Program for Online Systems," while simultaneously setting an example in its capacity as a host organization towards reform of the volatile VDP landscape in favor of security researchers.[20] The DOJ Framework outlines a high-level process for how an organization may structure a vulnerability disclosure program and advises host organizations on how to eliminate civil or criminal prosecution risk for security researchers that may arise from a poorly drafted policy.[21] Although the government is thought to lag behind innovative private sector companies in stature, federal agencies, unexpected first-adopters of fair VDP practices, have set the example for how organizations should operate VDPs.[22]

Several organizations in the private sector have taken public steps to reform their VDPs based on the DOJ's helpful guidance. However, after three years since the DOJ Framework's release, it has not had enough of an impact on private sector VDP reform. Given the changing landscape of U.S. government-run VDPs, which captures adequate process and protections for agency VDPs, this Note argues that there should be top-down pressure on the private sector to reform VDP policies and processes, using the DOJ's framework as a tool to do so.

Section I of this Note sets forth the VDP process, including actions taken by the host organization and researchers during VDP creation and the vulnerability lifecycle. Section II explores the current anti-hacking legal landscape and its impact on security research, including the role of safe harbor language. Section III explores the DOJ Framework in detail, highlighting why it is a useful tool towards reducing legal risks to security researchers through private sector VDP reform. Section IV outlines the U.S. government's unconventional adoption of VDPs, the recent call for mandatory and uniform VDPs at every government agency, and the influence the government has on private sector VDPs seen through commercial VDP platforms. Section V proposes that the DOJ Framework, if properly updated and maintained through a multi-stakeholder approach, has the potential to facilitate comprehensive standards in private sector VDPs, using the government's role in the VDP industry as used an exemplary metric that comports with the needs of both host organizations and security researchers alike.

---

19. *Id.*

20. *See generally* U.S. DEP'T OF JUST., A FRAMEWORK FOR A VULNERABILITY DISCLOSURE PROGRAM FOR ONLINE SYSTEMS (2017), https://www.justice.gov/criminal-ccips/page/file/983996/download [https://perma.cc/3C9X-NKUR] [hereinafter *DOJ Framework*].

21. *Id.*

22. *See* Dan Lohrmann, *Why Offering Bug Bounties Will Be Widespread, Even in Government*, GOV'T TECH., (July 16, 2017), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/why-offering-bug-bounties-will-be-widespread-even-in-government.html [https://perma.cc/7LXX-S7CY].

II. VULNERABILITY DISCLOSURE PROGRAMS IN PRACTICE: HOW DO THEY WORK?

Organizations most commonly utilize their permanent security operations teams to handle a range of cybersecurity issues in-house.[23] However, addressing vulnerabilities is a time and resource-intensive practice, and an organization aiming to employ long-term, preemptive measures to discover vulnerabilities may face challenges when trying to do so solely through in-house security.[24] For example, few organizations have adequate bandwidth to look for new bugs while mitigating existing ones.[25] Depending on the size of an organization or the number of systems under its ownership, vulnerability-related security issues may generate enough work for an entire business unit within the organization.[26] As a result, there is great incentive for organizations to encourage, reward, and develop relationships with external researchers who find security bugs in organizations' systems in real-time through VDP deployment.[27] When vulnerability hunting is left to a large and global community of external researchers, internal teams can better focus on fixing existing bugs, creating systems to better avoid bugs in the future, and handling other issues within the organization's security infrastructure.[28]

The VDP process ordinarily begins when an organization solicits security research services from the public by setting up an internal VDP.[29] The VDP creation process may vary in formality based on an organization's size, resources, and sophistication.[30] In creating a VDP, host organizations draft and enforce program terms and legal terms ("legal terms"),[31] which effectively serve as contracts between the security researcher and host

23. *See* MCKINSEY & CO., PERSPECTIVES ON TRANSFORMING CYBERSECURITY 20 (2019), https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx [https://perma.cc/WZ8V-965A].

24. *See* Thomas Maillart et al., *Given Enough Eyeballs, All Bugs Are Shallow? Revisiting Eric Raymond With Bug Bounty Programs*, 2 J. OF CYBERSECURITY 81, 88 (2017).

25. *See* Vincent Smyth, *Vulnerability Intelligence*, BCS, (Apr. 4, 2017), https://www.bcs.org/content-hub/vulnerability-intelligence/ [https://perma.cc/52CF-BANF].

26. *Id.*

27. Maillart et al., *supra* note 24, at 81.

28. *See* JASON PUBAL, SANS INSTITUTE INFORMATION SECURITY READING ROOM, BUG BOUNTY PROGRAMS: ENTERPRISE IMPLEMENTATION 2 (2020), https://www.sans.org/reading-room/whitepapers/application/bug-bounty-programs-enterprise-implementation-38250 [https://perma.cc/NF62-QQYU].

29. *See* J.M. Porup, *Bug Bounty Platforms Buy Researcher Silence, Violate Labor Laws, Critics Say*, CSO, (Apr. 2, 2020), https://www.csoonline.com/article/3535888/bug-bounty-platforms-buy-researcher-silence-violate-labor-laws-critics-say.html [https://perma.cc/4YGM-EDPP].

30. *Id.*

31. Program terms often include terms technical and instructional in scope, with formal legal terms included as part of the larger program terms. This Note collectively refers to host organization program terms and legal terms as "legal terms."

organization.[32] In general, security researchers take affirmative actions to manifest assent to contract terms upon submission of a vulnerability to a host's VDP, as well as click-through consent if they agree to a program's general program terms.[33]

The next step occurs when a security researcher discovers a vulnerability in the host organization's system.[34] After discovering a vulnerability, the security researcher reports the vulnerability to the host organization through the VDP.[35] If a security researcher discovers a valid bug, the company's legal terms dictate the next steps in the process regarding what the security researcher can do with their findings.[36] Some host organizations may allow for public disclosure of security research findings, with a prevailing norm that security researchers work closely with host organizations ahead of time to ensure remediation of the vulnerability before public disclosure to avoid unwanted exploit of the vulnerability found in good faith.[37] Other host organizations require confidentiality from security researchers to avoid reputational harm, a practice generally disfavored by the VDP community because host organizations may fail to capture the extent to which confidentiality is required.[38] Some security researchers may choose to publicly disclose a vulnerability without the permission of the host organization, a decision that comes with legal risks.[39] Researchers' risk tolerance often comes down to reputation and reward.[40]

Host organizations reward security researchers for their findings through recognition, professional opportunities, and monetary compensation—the "bounty" in the bug bounty program.[41] Many host organizations pay significant monetary rewards to researchers who discover

32. *See generally* Amit Elazari, *Hacking the Law: Are Bug Bounties a True Safe Harbor?*, ENIGMA, (Jan. 18, 2018), https://www.usenix.org/conference/enigma2018/presentation/elazari [https://perma.cc/9AC4-JY33] (video explaining importance of contractual terms in VDPs).

33. *See* Nguyen v. Barnes & Noble. Inc., 763 F.3d 1171 (9th Cir. 2014) (finding that browse-wrap contracts are generally enforceable in U.S. if sufficient notice is given); *See* RYAN ELLIS AND VIVEK MOHAN, REWIRED: CYBERSECURITY GOVERNANCE 252–53 (Ryan Ellis et al., eds., 2019).

34. *See* HOUSEHOLDER ET. AL., *supra* note 4, at 29.

35. *Id.*

36. *Id.* at 42.

37. *See id.* at 43; *see* Porup, *supra* note 29.

38. *See* Porup, *supra* note 29.

39. *See* Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753, 797 (2016).

40. *Id.* at 818.

41. *See* Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1061 (2011).

and disclose vulnerabilities in their systems.[42] According to HackerOne,[43] a VDP coordination service that connects security researchers to host organizations, security researchers earned almost $40 million in monetary rewards through the HackerOne platform alone in 2019, with six hackers surpassing $1 million in lifetime earnings.[44] More competitive programs run by companies like Google, Apple, and Microsoft offer individual bounties up to $1.5 million for critical issues.[45]

According to Kesan and Hayes, "[R]eputation is practically a currency in the information security field. Being known as the person who discovered a major security flaw might prove as valuable as being paid in legal currency."[46] Though some security researchers may bear legal risks in pursuit of recognition or reward, such risk tolerance is rarely sustainable, as organizations have a practice of suing or threatening to sue researchers who discover vulnerabilities in their systems, using broad anti-hacking laws to compel researcher fear and silence.[47]

III. THE CURRENT LEGAL LANDSCAPE: LEGAL RISKS FACED BY VDP SECURITY RESEARCHERS

The Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act (DMCA) are the primary laws that make up the anti-hacking legal landscape.[48] U.S. anti-hacking laws impose criminal and civil liabilities on certain forms of computer hacking to protect users, organizations, and government from malicious actors.[49] While anti-hacking

42. *See, e.g.*, *Chrome Vulnerability Reward Program Rules*, GOOGLE APPLICATION SEC., https://www.google.com/about/appsecurity/chrome-rewards/ (last visited Apr. 18, 2021) [https://perma.cc/QK69-3L77] ("Rewards for qualifying bugs typically range from $500 to $150,000. We have a standing $150,000 reward. . . ."). A bug bounty program is synonymous to a vulnerability disclosure program (VDP) as used in this context.

43. HackerOne is one of several commercial bug-bounty management platforms which help organizations build and maintain bug bounty programs. *See Company*, HACKERONE, https://www.hackerone.com/company (last visited Apr. 18, 2021) [https://perma.cc/ZEQ6-ND2W].

44. *See The Hacker-Powered Security Report 2020,* HACKERONE (Feb. 23, 2020), https://www.hackerone.com/resources/reporting/the-2020-hacker-report [https://perma.cc/6WRC-Y6WT]; *see Six Hackers Break Bug Bounty Record, Earning Over $1 Million Each On Hackerone*, HACKERONE, (Aug. 29, 2019), https://www.hackerone.com/press-release/six-hackers-break-bug-bounty-record-earning-over-1-million-each-hackerone [https://perma.cc/6S24-PKMJ].

45. *See Six Hackers Break Bug Bounty Record, Earning Over $1 Million Each On Hackerone*, *supra* note 44.

46. *See* Kesan & Hayes, *supra* note 39, at 794.

47. *See* Porup, *supra* note 29.

48. *See generally* 18 U.S.C. § 1030(a) (2012); 17 U.S.C. § 1201(a)(1)(A) (2012); *see also* Kesan & Hayes, *supra* note 39, at 792.

49. *See* Jenna McLaughlin, *Justice Department Releases Guidelines on Controversial Anti-Hacking Law*, THE INTERCEPT, (Oct. 26, 2016), https://theintercept.com/2016/10/26/justice-department-releases-guidelines-on-controversial-anti-hacking-law/ [https://perma.cc/X6SJ-QN8L].

laws intend to capture malicious hacking practices, they often fail to legitimize necessary security research practices used by researchers in VDPs.

Because of the robust VDP community, host organizations have a legitimate interest in insulating themselves from the risk that comes with soliciting security research from the general public.[50] Despite significant industry adoption of VDPs and the significant monetary rewards involved, there are no formal regulatory requirements to deploy VDPs.[51] As a result, the security research community falls victim to uncertainties about the legality of security research due to the failure to comply with program legal terms if such terms are too limiting, unclear, or improperly drafted.[52] Poorly crafted legal terms may subject a researcher to unknown liability, while overly-restrictive terms muzzle researchers and discourage research.[53]

A. The Computer Fraud and Abuse Act and Its Impact on Security Research

The CFAA criminalizes the intentional accessing of a "computer" without authorized access or by exceeding authorized access.[54] "Computer" is broadly defined to include virtually any system with Internet connectivity, including mobile devices.[55] The Second, Fourth, and Ninth Circuits interpret "exceeding authorized access" narrowly, limiting it to bypass of access controls or stealing of account data,[56] while the First, Fifth, Seventh, and Eleventh Circuits read the statute's phrase broadly to include the use of a computer for purposes prohibited in a terms of service agreement.[57] Without regulatory oversight over how host organizations implicate legal repercussions in their terms of service, interpretation of the CFAA's use of "authorization" falls to host organizations' contracts.[58] When combined with the lack of judicial consistency regarding the CFAA, security researchers must choose between the legal risks of running afoul of the CFAA under a broad interpretation or not conducting the research at all.[59]

The CFAA is inapt for modern uses of the Internet, causing widespread public confusion regarding the statute's application. Taking the realities of

---

50. *See* Porup, *supra* note 29 (referencing risk management concerns that may exist inside customer organizations).

51. *Id.*

52. *Id.*

53. *Id.*

54. *See* 18 U.S.C. § 1030 (2012).

55. *See* 18 U.S.C. § 1030(e).

56. *See* United States v. Valle, 807 F.3d 508 (2d Cir. 2015); WEC Carolina Energy Sols. v. Miller, 687 F.3d 199 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

57. *See* EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577 (1st Cir. 2001); United States v. John, 597 F.3d 263 (5th Cir. 2010); Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

58. Kirsch, *supra* note 14, at 399 (noting that it is commonplace for private entities to define and apply criminal activity as it exists under the CFAA).

59. *See* Joseph Lorenzo Hall & Stan Adams, *Taking the Pulse of Hacking: A Risk Basis for Security Research,* CTR. FOR DEMOCRACY & TECH. 9 (Mar. 2018), https://cdt.org/wp-content/uploads/2018/04/2018-03-27-Risk-Basis-for-Security-Research-FNL.pdf [https://perma.cc/85SP-5FLT].

security research into consideration, the uncertainties and inconsistent applications of the CFAA chill security research.[60] Even when a defendant's actions do not result in any financial loss or harm, a violation of the CFAA may lead to criminal penalties, including imprisonment.[61] According to a 2018 study conducted by the Center for Democracy and Technology (CDT) about the risk basis for security research, half of the subjects interviewed for the study reported the CFAA as a primary source of risk.[62]

In 2012, DOJ indicted security researcher Andrew Auernheimer for discovering an email breach in AT&T's servers by writing a program exposing the vulnerability, alerting victims of the breach, and disclosing email addresses obtained through the breach to a public news site.[63] DOJ charged Auernheimer with felony computer hacking under the CFAA in the U.S. District Court for the District of New Jersey, which sentenced him to 41 months in prison.[64] Auernheimer's conviction under the CFAA was based on "unauthorized access" to the system.[65] The finding that Auernheimer bypassed any authorizations—despite not using a password, login, or cookies—to access a publicly available website requires a dangerously broad reading of the CFAA.[66]

Auernheimer was able to reveal the vulnerability without using a password, login, or cookies—all actions which do not constitute a bypass of authorization in a technical sense, despite the court's interpretation of the CFAA.[67] In this case, AT&T did not employ protective measures to control access to the information obtained and disseminated by the defendant.[68] On appeal, Auernheimer argued that the company made the "information available to everyone and thereby authorized the general public to view the information," constituting authorized action under the CFAA.[69] The appeals

60. *Id.* ("Uncertainty potentially resulting in steep criminal penalties creates a significant chilling effect for researchers.").

61. *See* 18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(A).

62. *See* Lorenzo & Adams, *supra* note 59, at 9.

63. *See* United States v. Auernheimer, 748 F.3d 525, 529–31 (3d Cir. 2014).

64. *See* Matt Brian, *Andrew 'weev' Auernheimer Sentenced to 41 Months for Exploiting AT&T iPad Security Flaw*, VERGE, (Mar. 18, 2013), https://www.theverge.com/2013/3/18/4118484/andrew-weev-auernheimer-sentenced-att-ipad-hack [https://perma.cc/Y6US-PNY7].

65. *Id.*

66. A narrow view of the CFAA signals that access to a publicly available website is not "unauthorized access. 18 U.S.C. § 1030(a)(2)(C); *see* Pulte Homes, Inc. v. Laborers' Intern. Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011).

67. *See* Orin Kerr, *United States v. Auernheimer, and Why I Am Representing Auernheimer Pro Bono on Appeal Before the Third Circuit*, THE VOLOKH CONSPIRACY, (Mar. 21, 2013), http://volokh.com/2013/03/21/united-states-v-auernheimer-and-why-i-am-representing-auernheimer-pro-bono-on-appeal-before-the-third-circuit/ [https://perma.cc/KX3C-BC9L].

68. *See Auernheimer*, 748 F.3d at 529.

69. *See Orin Kerr's Appeal Brief for Andrew "Weev" Auernheimer – Another CFAA Case,* GROWKLAW (July 2, 2013), http://www.groklaw.net/articlebasic.php?story=20130702033515452 [https://perma.cc/8CR9-VFZL].

court eventually overturned the district court's ruling on technical grounds, leaving the CFAA's application to Auernheimer's activity unresolved.[70]

The vague interpretation of the CFAA in *Auernheimer* blurs the line between malicious hacking and security research activity.[71] The opinion suggests that the CFAA equates unrestricted access to a webpage like AT&T's with unauthorized access considered unlawful under the CFAA.[72] *Auernheimer* suggests that disclosure methods that entail sharing security flaw information publicly, the type of activity at the core of VDPs, may be subject to criminal penalty. Auernheimer's story creates an uncertain environment for security research, making security researchers wary about disclosing security vulnerabilities following the case's broad application of the CFAA.

B. The DMCA and Its Impact on Security Research

Section 1201(a) of the Digital Millennium Copyright Act (DMCA), the anti-circumvention provision of copyright law, forbids the unauthorized bypass of certain technological boundaries controlling access to software or code protected by copyright.[73] Section 1201(a) does not explicitly differentiate between circumvention of technological boundaries that infringe copyright and circumvention for legitimate reasons, such as authorized security research.[74] Security researchers concerned about the legal risks posed by a potential violation of the DMCA tend to shy away from performing research on systems protected by access controls.[75]

A statutory exemption for security research under the DMCA was extended in 2018, allowing for "good-faith" security research.[76] However, among other limitations, the exemption requires that the research will not violate any applicable law, including the CFAA and contract law.[77] Under this requirement, legal terms continue to ban, either implicitly or by way of poor drafting, researchers from "circumvention" techniques that may be necessary to properly perform security research. Paradoxically, the exemption is meaningless unless VDP terms of use allow for circumvention and establish authorized access under the DMCA, as well as by implication under the

70. *See Appeals Court Overturns Andrew "weev" Auernheimer Conviction*, ELEC. FRONTIER FOUND. (Apr. 11, 2014), https://www.eff.org/press/releases/appeals-court-overturns-andrew-weev-auernheimer-conviction [https://perma.cc/2DZT-53HA].

71. Kirsch, supra note 14, at 394.

72. *Id.*

73. *See* 17 U.S.C. § 1201.

74. *See generally id.*; Stan Adams, *Getting Better All the Time: Security Research and the DMCA*, CTR. FOR DEMOCRACY & TECH., (Oct. 26, 2018), https://cdt.org/insights/getting-better-all-the-time-security-research-and-the-dmca/ [https://perma.cc/D5CV-PDRY].

75. *See* Hall & Adams, *supra* note 59, at 6–7.

76. *See* 17 U.S.C. § 1201(j)(1).

77. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944, 65956 (Oct. 28, 2015) (to be codified at 37 C.F.R. pt. 201).

CFAA.[78] Because many researchers have an incomplete understanding of the conditions for eligibility, the DMCA continues to chill security research.

C. *Safe Harbor Language: A Superficial Fix, Not a Complete Solution*

Adequate safe harbor language in contracts would authorize research in light of anti-hacking laws such as the CFAA and DMCA by including a clearly defined scope of when authorization may occur.[79] However, safe harbor language is the exception and not the rule across VDPs.[80]

But even when safe harbor language exists, it may be an inadequate solution for liability posed to researchers, partly because a host organization may write VDP terms to determine, in its sole discretion, if a security researcher meets the safe harbor criteria. The possibility of this power imbalance, even in the presence of an adequate safe harbor, limits the comfort researchers can take in the presence of safe harbor terms.[81] This power imbalance is not merely hypothetical, but rather a regular practice in the VDP industry today. Some organizations ask security researchers to enter into a series of agreements, in addition to the VDP program terms, as a prerequisite to VDP participation, threatening prosecution under the CFAA if the NDA is refused. For example, PayPal asks security researchers to agree to an NDA as part of their terms and agreements, agreeing not to bring private action or refer a matter for public inquiry only when the security researcher meets all the guidelines of the terms and agreements.[82] Further, platforms like HackerOne openly acknowledge that safe harbor terms offered by host organizations running programs on their platform may be contingent on program terms, including an NDA.[83]

In March of 2020, a blockchain-based voting company, Voatz, referred a student researcher to the FBI over what the company claims was an attempted intrusion by the security researcher.[84] Voatz touts a safe harbor statement as part of its VDP program. Following the criticism and negative reporting following the incident, Voatz retroactively changed its VDP program terms by narrowing the scope of its safe harbor policy and negating full legal protection.[85] Voatz serves as an example of how even a safe harbor may derail the environment of trust between researchers and the host

78. *See* 17 U.S.C. § 1201.

79. *Id.*

80. *See generally Photo Gallery*, AMIT ELAZARI, https://amitelazari.com/#legalbugbounty-hof (last visited Jan. 24, 2020).

81. *See* Porup, *supra* note 29.

82. *See e.g.*, *Paypal - Bug Bounty Program*, HACKERONE, https://hackerone.com/paypal (last visited Jan. 24, 2020) [https://perma.cc/SG57-WAJ2].

83. *See generally Vulnerability Disclosure Guidelines*, HACKERONE, (July 29, 2019), https://www.hackerone.com/disclosure-guidelines [https://perma.cc/3G5M-2Z9R].

84. *See* Yael Grauer, *Voatz Bug Bounty Kicked Off of HackerOne Platform*, COINTELEGRAPH, (Mar. 31, 2020), https://cointelegraph.com/news/voatz-bug-bounty-kicked-off-of-hackerone-platform [https://perma.cc/4A3J-74NU].

85. *Id.*

organization. For safe harbor provisions to work, host organizations must follow their own protocol.

IV. THE DOJ'S DISCRETIONARY GUIDANCE FOR PRIVATE VDPS

In July 2017, the Department of Justice (DOJ) Cybersecurity Unit[86] released a framework outlining guidelines for host organizations to use security research to identify bugs in their systems through VDPs.[87] The DOJ Framework emphasizes the clear boundaries necessary when hosting a VDP to reduce violations under the CFAA and DMCA.[88] The DOJ Framework recognizes the risks associated with careless or overbroad policy language and provides guidance on how adequate VDP procedures may address the range of legal risks involved in running and participating in VDPs.[89] The DOJ Framework does not mandate specific requirements or objectives for vulnerability disclosure but encourages organizations to protect security researchers through their terms, procedures, and processes.[90] Rather, the DOJ Framework is intended to help host organizations effectively run VDPs through standard practices and policies.[91]

The DOJ Framework offers a four-part roadmap of guidelines for host organizations to follow.[92] For example, the DOJ Framework points to templates for VDP creation, provides guidelines for communicating with security researchers, and advises on the adoption of a multi-stakeholder process when designing a VDP.[93] All four steps delineated by the DOJ Framework address, among other things, the importance of safe harbor language.

Dr. Amit Elazari, a prominent scholar in the Bug Bounty and VDP space, compiled an initial list of VDPs that adopt language in adherence with the DOJ Framework's guidance on legal safe harbors for security research.[94]

---

86. The DOJ is responsible agency for CFAA strategy and enforcement. *Cybersecurity Unit*, U.S. DEP'T OF JUST., https://www.justice.gov/criminal-ccips/cybersecurity-unit (last updated Mar. 12, 2020) [https://perma.cc/69QD-XP76].

87. *See DOJ Framework*, *supra* note 20.

88. *Id.* Application to DMCA is implied based on the relationship between the CFAA and DMCA.

89. *Id.* When organizations take the time to establish clear boundaries and unambiguous protocols through their program's policy language, they are more likely to avoid the risks associated with unauthorized security research.

90. *Id.*

91. *Id.* at 1, n.3 ("This guidance is intended as assistance, not authority such that nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter."); *see e.g.*, United States v. Caceres, 440 U.S. 741 (1979); Ellen S. Podgor, *Department of Justice Guidelines: Balancing "Discretionary Justice"*, 13 CORNELL J.L. & PUB. POL'Y 167, 169 (2004) ("Courts routinely find these guidelines strictly internal an d unenforceable at law. [Failure to follow guidelines] cannot be used by the accused . . .").

92. *See id.*

93. *DOJ Framework*, *supra* note 20.

94. *See Photo Gallery*, *supra* note 80; *see generally Public Bug Bounty List*, BUGCROWD, https://www.bugcrowd.com/bug-bounty-list/ (last visited Mar. 22, 2020).

Based on her findings, as of March 2018, 26 VDPs adopted language that follows the DOJ Framework's guidelines on the legal safe harbor. Due to the publication of a safe harbor directory maintained by Disclose.io, there is now a comprehensive and up to date list of VDPs.[95] As of December 2019, 106 of the 311 total VDPs included as part of Disclose.io's comprehensive list of public VDPs successfully include full safe harbors.[96] While qualitative or quantitative research on the correlation between the DOJ Framework does not currently exist, the increase in VDPs with full safe harbors is significant, increasing four-fold in under two years.[97] Academics and security researchers have long advocated for VDP safe harbors, but the release of the DOJ Framework provides a tangible and trustworthy model for host organizations to utilize in writing or reforming VDP policies.

The DOJ Framework provides much more than guidelines for standardizing safe harbor language, which may not be sufficient to fully insulate security researchers from legal risks, as discussed in Part II. The DOJ Framework is meant to help focus host organizations' attention on knowing the risks they face based on their size, resources, and involvement with the researcher community.[98] In sum, the DOJ Framework provides holistic yet flexible guidelines for host organizations to use when considering the efficacy of their VDPs.[99]

The DOJ Framework is a resource for organizations running VDPs, offering a comprehensive form of guidance for host organizations.[100] While it does not mandate legal terms or practices that eliminate or clarify legal risks associated with security research on privately owned systems, it provides the tools to help host organizations do so.[101]

Some organizations have, in response to the DOJ Framework, successfully adopted direct commitments related to restricting legal actions, while other organizations have gone so far as to adopt policy language that legally authorizes access under existing anti-hacking laws. In fact, the government's own VDPs across agency host organizations exemplify the very standards the DOJ Framework aims to socialize, highlighting that the DOJ Framework is not the government's only contribution to the VDP landscape.

V. THE U.S. GOVERNMENT'S INFLUENTIAL ROLE IN VDP GOVERNANCE

Cyberattacks and data breaches do not discriminate. The risk of sweeping financial and reputational damage exists in both the private and

95. *See Public Bug Bounty List*, *supra* note 94.

96. *Id.* 106 out of 311 total VDPs documented on the list is maintained as part of the Disclose.io Safe Harbor project.

97. *Id.*

98. *See generally DOJ Framework*, *supra* note 20

99. *See id.*

100. *See generally Caceres*, 440 U.S. 741.

101. *See e.g.*, *DOJ Framework*, *supra* note 20.

public sectors.[102] The private sector has long crowdsourced vulnerabilities, whereas the U.S. federal government only recently began employing VDPs at the federal agency level.[103] However, VDPs are considered an industry best practice not only in the private sector, but for governments as well.[104] U.S. government-run VDPs distinguish themselves from those in the private sector by providing ethical hackers clear guidelines for submitting bugs found in government systems.[105]

A. The U.S. Government as a "Crowdsourcer": Validating the Importance of Public Engagement to Cybersecurity

The government adopted its first VDP in April 2016 with the Department of Defense's (DOD) "Hack the Pentagon" program.[106] The government's entry into the private sector-dominated VDP world signaled widespread recognition of citizen engagement as a beneficial way to address cybersecurity challenges.[107] The DOD's pilot program exceeded expectations, resulting in over 1,000 vulnerability reports,[108] which the DOD explained would normally take hundreds of hours of internal manpower at a cost above $1 million for the agency without a VDP.[109] The entire cost of the pilot was $150,000, with about half of that amount going to security researchers in payouts.[110] In November 2016, the DOD ran its second program, "Hack the

102. *See* Sarah A. Lafen, *U.N. Regulation - The Best Approach to Effective Cyber Defense?*, 45 SYRACUSE J. INT'L L. & COM. 249, 250 (2018).

103. *See* Sean Martin, *History And Interesting Facts About Bug Bounties - An Appsec Usa 2017 Panel Recap*, ISTP MAGAZINE, Sept. 23, 2017, https://www.itspmagazine.com/itsp-chronicles/history-and-interesting-facts-about-bug-bounties-an-appsec-usa-2017-panel-recap [https://perma.cc/SD6K-KC3N] (noting that the private sector is where the VDP industry was first born, with Netscape launching the first known bug bounty program in 1995. Netscape was very much ahead of its time. Many companies like Google and Microsoft did not launch bug bounty programs until the 2010s. In xthe past decade, growth of the industry has mushroomed).

104. *See The Hacker-Powered Security Report 2019,* HACKERONE (Dec. 3, 2019), https://www.hackerone.com/resources/reporting/the-hacker-powered-security-report-2019 [https://perma.cc/ZGY2-L72D].

105. *See* Lindsey O'Donnell, *U.S. Agencies Must Adopt Vulnerability-Disclosure Policies by March 2021*, THREATPOST (Sept. 2, 2020), https://threatpost.com/u-s-agencies-vulnerability-disclosure-policies-march-2021/158913/ [https://perma.cc/2EPY-W9QP].

106. Press Release, Department of Defense, Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program (Oct. 24, 2018) https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/ [https://perma.cc/6RNU-57BV].

107. *See* Ines Mergel, *Social Media Adoption and Resulting Tactics in the U.S. Federal Government*, 30 GOV'T INFO. QUARTERLY 123, 130 (2013).

108. *See "Hack the Pentagon" Fact Sheet*, U.S. DEP'T. OF DEF., (Jun. 17, 2016), https://dod.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf [https://perma.cc/S9SW-U25T].

109. *See* Lisa Ferdinando, *Carter Announces 'Hack the Pentagon' Results*, U.S. DEPT. OF DEF., (Jun. 17, 2016), https://www.defense.gov/Explore/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results/ [https://perma.cc/LSM5-ZQW3].

110. *See id.*

Army," through which hackers received $100,000 in total payouts.[111] In conjunction with the "Hack the Army" program, the DOD announced a "Digital Vulnerability Disclosure Policy," providing guidance to security researchers on legal boundaries for testing and disclosing vulnerabilities in DOD websites.[112] Prior to the DOJ's release of its framework, the DOJ's Criminal Division was consulted in the development of this policy language to help the DOD carry out its commitment to working "openly and in good faith with researchers."[113]

The DOD's consistent use of VDPs, while a departure from traditional security strategies employed by the agency, has produced favorable outcomes backed by quantitative evidence and established a route for the government to tap into private sector cybersecurity talent.[114] Following the positive response to the DOD's Hack the Pentagon program, other agencies began to develop similar programs, including the Department of State, Food and Drug Administration (FDA), General Services Administration (GSA), and Department of Homeland Security (DHS).[115] In December 2018, President Donald Trump signed the SECURE Technology Act (H.R. 7327) into law, which required the DHS to establish a security vulnerability disclosure policy and establish a VDP program.[116] The passage of the SECURE Technology Act signals Congress' recognition of the value of VDPs in the context of the government.[117]

B. The U.S. Government as a "Rule Maker": The DHS' Compulsory Authority over Government VDPs

On November 27, 2019, the DHS released the Cybersecurity and Infrastructure Security Agency's (CISA) draft Binding Operational Directive 20-01 ("the DHS Directive") titled "Develop and Publish a Vulnerability

111. *See* Michael Mimoso, *Hack the Army Bounty Pays Out $100,000; 118 Flaws Fixed*, THREAT POST, (Jan. 20, 2017), https://threatpost.com/hack-the-army-bounty-pays-out-100000-118-flaws-fixed/123216/ [https://perma.cc/Q6BN-X98J].

112. *See DOD Announces Digital Vulnerability Disclosure Policy and "Hack the Army" Kick-Off*, U.S. DEP'T. OF DEF., (Nov. 21, 2016), https://www.defense.gov/Newsroom/Releases/Release/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/ [https://perma.cc/RFE8-ZGJV].

113. *Id.*

114. *See, e.g.*, *The Hacker-Powered Security Report 2019*, HACKERONE 11 (Dec. 3, 2019), https://www.hackerone.com/resources/reporting/the-hacker-powered-security-report-2019 [https://perma.cc/4Q2S-DZ94] (highlighting that as of December 2019, the DOD has detected more than 10,000 researcher-discovered security vulnerabilities over the short lifespan of its multiple VDPs).

115. *Id.*

116. *See* SECURE Technology Act, H.R. 7327, 115th Cong. (2018); THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [https://perma.cc/LSX6-YZRQ] (finding that the White House is centrally responsible for the political and strategic management and coordination of cybersecurity policies through the National Security Council).

117. *See generally* H.R. 7327.

Disclosure Policy."[118] The DHS Directive requires every federal agency to run a VDP, mandating the creation of a formal process for researchers to report vulnerabilities within the agency's public-facing websites or information technology infrastructure, and a system for addressing vulnerabilities discovered through the VDP.[119] The DHS Directive calls for each agency to set standardized vulnerability disclosure policies,[120] which will help promote the establishment of clear boundaries around the legalities of hacking government systems. The DHS Directive effectively mandates agencies to bring themselves up to speed within six months with a VDP and disclosure policy and requires that all internet-accessible systems and services are in the scope of the policy by the two-year mark.[121] The DHS Directive, which was open for public comment until December 27, 2019, specifically outlines the principles that each agency's VDP must contain, including language that requires agency programs to delineate legal protections for researchers, the scope of agency assets open to program participants, and guidelines for how the agency will resolve reported bugs.[122]

C. The Government as an "Example": The Impact of Government VDPs on the Private Sector, as Evidenced Through Commercial VDP Management

When the DOD launched the first known government VDP, "Hack the Pentagon," the effort was outsourced to HackerOne, which not only operated the initiative, but also advised the DOD on the creation and growth of the program.[123] Since 2016, the DOD has worked with HackerOne on programs like "Hack the Army," "Hack the Airforce," "Hack the Marine Corps," as well as future iterations of "Hack the Pentagon."[124] A partnership between

---

118. *See* Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, Binding Operational Directive 20-01: Develop and Publish a Vulnerability Disclosure Policy (Sept. 2, 2020).

119. *Id.*

120. *Id.*

121. *Id.*

122. *See* Sean Lyngaas, *DHS Is Mulling an Order That Would Force Agencies to Set Up Vulnerability Disclosure Policies*, CYBERSCOOP, (Oct. 23, 2019), https://www.cyberscoop.com/dhs-vulnerability-disclosure-program-bod/ [https://perma.cc/28N2-KVU8]; Develop and Publish a Voluntary Disclosure Policy, 84 Fed. Reg. 69,761 (proposed Dec. 13, 2019).

123. Press Release, NewsWire, Department of Defense Launches Bug Bounty Program on HackerOne (Mar. 31, 2016), https://www.newswire.com/news/department-of-defense-launches-bug-bounty-program-on-hackerone [https://perma.cc/SGK3-5VQM].

124. *See* Marten Mickos, *The Best Is Yet to Come: DoD Awards New Hack the Pentagon Program to HackerOne*, HACKERONE (Oct. 24, 2018), https://www.hackerone.com/blog/Best-Yet-Come-DOD-Awards-New-Hack-Pentagon-Contract-HackerOne [https://perma.cc/NHU7-LP6L]. More recently, the U.S. General Services Administration's Technology Transformation Service also signed a contract with HackerOne for the first bug bounty program run by a civilian federal agency. Tajha Chappellet-Lanier, *GSA Awards $2M Bug Bounty Service Contract to HackerOne*, HACKERONE (Sept. 1, 2018), https://www.fedscoop.com/gsa-hackerone-bug-bounty-contract/ [https://perma.cc/X27F-9AZF].

HackerOne, a private sector startup in its nascent stages, and the DOD, arguably the most security-aware organization in the nation, signals a great deal of credibility and value housed in the use of commercial platforms for VDP management.[125]

The credibility implied in HackerOne's contracts with multiple government agencies, as well as the use of the DOD's VDP as a successful model suggests to the private sector that commercial VDP platforms can accommodate the needs of large, complex enterprises. As a result, many of the largest private companies, including household names like Goldman Sachs, General Motors, Uber, Starbucks, and many others, have signed on to work with platforms trusted by the government.[126] Organizations of all sizes find commercial VDP platforms attractive because experienced third parties assist every step of the process, including writing a policy, setting a scope, and establishing bounties.[127]

Industry use of commercial vendors in VDP management shows the influence of the DOJ Framework, as seen in agreements from companies like HackerOne.[128] Among their many DOJ-Framework-aligned recommendations,[129] HackerOne's "Vulnerability Disclosure Guidelines" include a "Safe Harbor" section which highlights that HackerOne is better able to protect, or help protect, security researchers in difficult disclosure situations if the security researcher's actions comport with the guidelines.[130] While not every organization on the HackerOne platform complies with DOJ Framework guidelines or even the safe harbor language, HackerOne's explicit support for researchers who comply with the DOJ Framework sets a floor for non-compliant VDP host organizations. As a result, a greater number of researchers who feel more comfortable pursuing VDPs contained on HackerOne (as compared to host organizations that run VDPs independently)

---

125. In addition to multiple contracts with U.S. federal government agencies, the European Commission and Singapore's Ministry of Defence (MINDEF) selected HackerOne for their bug bounty programs. The implementation of the Directive signals a trend towards the use of HackerOne and its competitors by a broader range of government agencies, especially those with limited security teams in need of support starting and running mandatory VDPs. *See generally Ministry of Defence, Singapore (MINDEF) Bolsters Security With Second HackerOne Bug Bounty Challenge*, HACKERONE (Sep. 27, 2019), https://www.hackerone.com/press-release/ministry-defence-singapore-mindef-bolsters-security-second-hackerone-bug-bounty, (last visited Nov. 1, 2020) [https://perma.cc/Z5C7-8RGW].

126. *See Goldman Sachs*, HACKERONE, https://hackerone.com/goldmansachs (last visited Jan 24, 2020) [https://perma.cc/VL5R-2U3S]; *General Motors*, HACKERONE, https://hackerone.com/gm (last visited Jan 24, 2020) [https://perma.cc/AEQ5-W7LQ]; *Uber*, HACKERONE, https://hackerone.com/uber (last visited Jan 24, 2020) [https://perma.cc/UP7X-3C36]; *Starbucks*, HACKERONE, https://hackerone.com/statbucks (last visited Jan 24, 2020).

127. *See generally Hacker-Powered Security for StartUps*, HACKERONE (2019), https://www.hackerone.com/resources/e-book/hacker-powered-security-for-startups (last visited Jan. 25, 2020).

128. *See generally Vulnerability Disclosure Guidelines*, https://www.hackerone.com/disclosure-guidelines (last updated July 29, 2019) [https://perma.cc/A268-F3X2].

129. *See generally id.*

130. *Id.*

are likely to flock to the platform. This creates quasi-network effects that draw in host organizations to partner with the platform given the breadth and quality of participating security researchers.

Commercial VDP platforms do not shy away from supporting and encouraging the use of the DOJ Framework, though there is little they can do beyond ensuring that their guidance to clients and overall philosophy align with the recommendation delineated in the framework. While commercial VDP platforms have researcher interests and safety in mind, they must balance their advocacy with the marketing of their services as part of a two-sided market.

VI. THE PATH FORWARD: RECOMMENDATIONS FOR STANDARDIZING PRIVATE SECTOR VDPS USING THE U.S. GOVERNMENT AS AN EXAMPLE

Commercial VDP platforms provide just one of many examples of the private sector looking to the government as a model for running an effective VDP. The credibility and influence of the government in the commercial VDP platform environment is only a snapshot of the VDP industry—one that not all host organizations in the private sector are influenced by. Thus, given current threats to the security research community posed by anti-hacking laws,[131] it is clear that inaction at the private sector level is not a viable option.

This Note argues that the DOJ Framework, combined with the U.S. government's exemplary use of and leadership in VDPs, has the potential to bridge the gap between managing the risks faced by both host organizations and security researchers. However, in its current state, the DOJ Framework is left largely ineffective and many private sector host organizations ignore it. The extensive guidance on strengthening VDP and cybersecurity practices put forth by the DOJ Framework and other regulatory agencies encourage host organizations to make a good faith effort to operate within the DOJ Framework to "stand a better chance if potential legal action" were to result from a cybersecurity incident.[132] While a segment of the VDP community recognizes the DOJ Framework as a step in the right direction, many important considerations about how the DOJ Framework will be used to improve the security research landscape on a wide scale have not been fully evaluated.

Operating within the DOJ Framework and taking advantage of the U.S. government's exemplary use of and leadership in VDPs can be achieved through a culmination of tactics aimed at ensuring that the DOJ Framework

131. *See* Riana Pfefferkorn, *The Importance of Protecting Good-Faith Security Research*, CTR. FOR INTERNET & SOC'Y, (Sept. 14, 2020), https://cyberlaw.stanford.edu/blog/2020/09/importance-protecting-good-faith-security-research [https://perma.cc/5AVK-AQKK]. Application to DMCA is implied based on the relationship between the CFAA and DMCA.

132. *See John K. Higgins*, *DoJ Calls On Private Sector to Strengthen Cybersecurity*, E-COMMERCE TIMES, (May 20, 2015), https://www.ecommercetimes.com/story/82079.html [https://perma.cc/9PMN-BEUY].

evolves alongside the VDP industry. This Note proposes two sustainable tactics for reforming private sector VDPs based on evaluating government and private sector VDPs, the anti-hacking landscape, and evolving cybersecurity practices. First, the private sector can achieve increased adoption of the DOJ Framework by mirroring the flexibility of existing effective cybersecurity standards. Second, the private sector must prioritize researchers' interests, exemplified by the DHS Directive and agency VDPs.

A. Compulsory DOJ Framework: Promoting Reform of Private Sector VDPs Through the Use of Standards

While mandating compliance with the DOJ Framework across private sector VDPs may be possible, few U.S. cybersecurity laws promulgate the authority to mandate private sector practices. Instead, Congress could pass legislation mandating uniform legal terms or standard VDP practices for host organizations, giving researchers the ability to conduct security research without fear of legal repercussions. Such regulation could shift the burden of ensuring that the policy language of the VDP, including the boundaries of both research activity and disclosure, adequately protects researchers participating in VDP programs in good faith. However, the need for government intervention in the form of mandated and standard language across host organizations is paternalistic and unnecessary. It is therefore in the private sector's best interest to allocate resources to secure sensitive information and maintain security.

A one-size-fits-all mandate for how a VDP must protect both researchers and host organizations is an unrealistic goal, even with the DOJ Framework's guidance. While mandatory standardization is a reality across U.S. civilian agencies, the DHS Directive is operated within a narrower scope, on a smaller scale, and based on VDP successes experienced by the DOD and its successors. When this methodology is transferred to the private sector, where VDPs vary in size, scope, resources, and experience, the success rate is much lower. In turn, cybersecurity standards, which are important in developing risk management strategies and effective security practices by establishing common approaches and requirements, are more realistic than mandatory compliance rules when it comes to socializing the DOJ Framework's practices across private sector VDPs.

Cybersecurity standards are created with the industry's needs in mind and usually include a multi-stakeholder approach involving consultation with industry, academia, regulatory bodies, and the public.[133] Cybersecurity standards are especially influential because of their ability to impact industries and markets as a whole. For example, in 2013, the National Institute of Standards and Technology (NIST), created the NIST Cybersecurity Framework, which is often perceived as a de facto standard in

133. 1 EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, GOVERNANCE FRAMEWORK FOR EUROPEAN STANDARDISATION 19 (2015), https://www.enisa.europa.eu/publications/policy-industry-research/at_download/fullReport.

cybersecurity.[134] The NIST Framework is highly influential not only in the U.S. but across many other jurisdictions that rely on it as a best practice.[135] The NIST Framework, like the DOJ Framework, is a set of industry standards and best practices for organizations in the management of cybersecurity risks, practices, and operations.[136] Before its release in 2013, NIST underwent an extensive consultation period during which it worked across sectors and industries in a public-private partnership.[137] In 2017, NIST reaffirmed the matters in the original framework, as well as its commitment to implementing the nation's cybersecurity goals.[138]

Like the NIST Framework, the DOJ Framework is capable of spearheading standardized compliance with baseline VDP guidelines through collaboration with the U.S. government to improve the VDP process. The legal terms and incentives presented to researchers correlate to the effectiveness of VDPs, with clear legal terms creating an attractive marketplace for vulnerabilities. For VDPs to operate as a marketplace for vulnerabilities, program terms must be clear and unambiguous. It becomes difficult for security researchers to navigate the rules and restrictions set out by host organizations when those rules are unclear.[139]

The U.S. government has not updated the DOJ Framework since its July 2017 release, though the VDP industry is changing rapidly. Companies around the world regularly launch new VDPs, not only to stay up to date on industry cybersecurity trends but also as reputational tools signaling trustworthiness to customers.[140] Existing host organizations regularly announce significant payouts, exemplified by Google Android's VDP, which recently offered a $1.5 million bounty for a researcher to find a specific Pixel-related exploit.[141] With a constant stream of VDP engagement in both the private and public sectors globally, the DOJ must reaffirm its commitment to its guidelines and make appropriate updates to best facilitate the private sector governance set forth by the framework. NIST's stakeholder engagement efforts played a role in the success of the NIST Framework, and its widespread adoption is likely a result of the consultative process and cross-industry consensus building.[142] A potential solution is increased DOJ

134. *See* Shin-yi Peng, *"Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime*, 51 CORNELL INT'L L.J. 445, 458 (2018).

135. *Id.*

136. *Id.* at 451.

137. *Id.*

138. *Id.* at 452.

139. 1 EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, *supra* note 133, at 5.

140. *See, e.g.*, Adam Bannister, *Bug Bounty Radar // November 2019,* THE DAILY SWIG, (Nov. 29, 2019), https://portswigger.net/daily-swig/bug-bounty-radar-november-2019 [https://perma.cc/99MW-HMGE].

141. *See* Corinne Reichert, *Google's Android Bug Bounty Program Will Now Pay Out $1.5 Million*, CNET, (Nov. 21, 2019), https://www.cnet.com/news/googles-android-bug-bounty-program-will-now-pay-out-1-5-million/ [https://perma.cc/26X6-W276].

142. *See* Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 328 (2015).

engagement with private sector stakeholders, a process that would necessitate private sector VDP players to acknowledge the DOJ Framework. This may encourage private sector stakeholders to voice concerns about the DOJ Framework instead of ignoring its guidance and potentially running a VDP which puts researchers at risk. It is not clear if the DOJ consulted stakeholders before the initial framework release in 2017. However, this Note argues that some degree of involvement in updating and implementing the framework's standards alongside a variety of stakeholders, mirroring the NIST Framework as a successful cybersecurity standard, is an instrumental step towards reforming VDP practices in the private sector.

B. Mirroring the DHS Approach: The U.S. Government as an Example in Responding to Concerns that the Private Sector Fails to Address

The government's rapid involvement in VDPs and adoption of the DHS Directive across all civilian agencies shows that the government's VDP practices are particularly exemplary when it comes to limiting liability risks faced by security researchers. The government's actions in the VDP space explicitly address the harms of poorly crafted legal terms and program policies, which cause security researchers to violate anti-hacking laws merely by participating in the program.

DHS's rationale behind the creation of its DHS Directive as a standard for a government-wide VDP [143] was to promote VDP participation by making it relatively easy, explaining that when "things [are] easier to do, more people will do them."[144] Like the DOJ Framework, the DHS Directive aims to make VDP expectations clear to reduce the complexities that come with security research.[145] To address concerns at the host organization level about how to implement these changes, DHS shared a draft VDP template and guidance for agencies to follow regarding the implementation of their respective VDPs.[146]

As part of the effort to stand up the DHS Directive, DHS explicitly recognized security researchers' main frustrations, including fear of legal action.[147] The Office of the Federal Chief Information Officer announced that government agency VDPs must, according to the DHS Directive, legally insulate those who come forward with vulnerabilities, citing clear differentiation "between acceptable and unacceptable means of gathering

143. *See* Jack Corrigan*, CISA Wants a Vulnerability Disclosure Program At Every Agency*, NEXTGOV, (Nov. 27, 2019), https://www.nextgov.com/cybersecurity/2019/11/cisa-wants-vulnerability-disclosure-program-every-agency/161586/ [https://perma.cc/CX7S-5LLP].

144. *See* Jeanette Manfra, *Improving Vulnerability Disclosure Together,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENC., (Nov. 27, 2019), https://www.cisa.gov/blog/2019/11/27/improving-vulnerability-disclosure-together [https://perma.cc/5QMK-J5QD].

145. *Id.*

146. *Id.*

147. *See* Liam Tung, *US to Order Every Federal Agency to Establish Own Bug Reporting Program in 2020,* CSO, (Nov. 29, 2019), https://www.csoonline.com/article/3500742/us-to-order-every-federal-agency-to-establish-own-bug-reporting-program-in-2020.html.

security" as the way to provide legal cover.[148] Through the DHS Directive, agency VDPs are mandated to provide assurances that good faith security research is not only welcomed but also authorized.[149] The DHS Directive calls on agency VDPs to clearly articulate the systems which are within the scope of vulnerability research activity.[150] If VDPs comply with the DHS Directive's call for clarity, security research is more likely to occur on selected systems in an authorized manner while avoiding unauthorized security research on systems where it is not solicited.

While it is generally uncommon for the government to lead in the information technology space, government agencies operate extremely progressively within the scope of VDPs based on a proven approach to security research.[151] The call for comprehensive and uniform practices across agency VDPs helps protect and incentivize security research at the governmental level amid the volatile anti-hacking legal landscape.

The DOJ should work closely with its counterparts at DHS, as well as across government agencies, to identify the challenges involved in standardization of the VDP process and legal terms on a more defined scale. VDPs are, by nature, premised on the idea of transparency. It is likely that the DHS, through its central oversight of all U.S. federal government VDPs, plans to release detailed qualitative and quantitative information regarding the results of mandatory government agency VDP implementation. The DHS Directive sets forth precise requirements for agencies developing and publishing vulnerability disclosure policies, in addition to rules on how to handle procedure, reporting, and researcher communications. The DOJ, which must also comply with DHS requirements and create a VDP of its own, should extract relevant takeaways and apply them to update the DOJ Framework. Based on the outcomes of the DHS Directive, the DOJ should set forth a parallel process of developing specific terms for industry-specific applications in the private sector. In this hypothetical, the DOJ may have more influence over standardization of VDP processes and terms if the framework is tailored to specific industries, especially those with organizational complexities and higher risks for non-compliance (e.g., financial services).

The private sector and government VDP markets are natural complements given the importance of access to and dissemination of cybersecurity information. A high bounty offered by any VDP industry participant for a specific bug sends a message to both the government and the private sector about the importance of addressing the vulnerability and sharing the results.[152] VDPs create information channels by which

148. Memorandum from Russel T. Vought, Director, Off. Mgmt. & Budget to the Heads of Executive Departments and Agencies (Sept. 2, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf [https://perma.cc/2HAW-T7CG].

149. Manfra *supra* note 144.

150. *Id.*

151. *See White Hat Hackers Help Pentagon Close Its Cybersecurity Holes*, DICE (Mar. 18, 2020), https://insights.dice.com/2020/03/18/white-hat-hackers-help-pentagon-close-its-cybersecurity-holes/ [https://perma.cc/GNJ3-MQ8Q].

152. *See* Serge Egelman et al., *Markets for Zero-Day Exploits: Ethics and Implications*, NEW SEC. PARADIGMS WORKSHOP 41, 44–45 (2013).

organizations can achieve partial objectivity in understanding cybersecurity risks through the successes and improvements experienced by other host organizations, including governments.

While the DOJ Framework may not have binding authority through its VDP guidelines, it establishes the presence of the U.S. government as a model player in the world of VDPs. The U.S. government has an immense interest in encouraging sound practices in the private sector to keep researchers excited and motivated about their participation in VDPs. In sum, through the DHS Directive and practices at agency VDPs, the government has identified steps to maintain the interest of security researchers, and the private sector should mirror this approach by using the DOJ Framework as a standard tool.

VII. CONCLUSION

VDPs are rooted in the idea that "given enough eyeballs, all bugs are shallow."[153] Consequently, the more researchers involved in identifying weaknesses in a host organization's systems, the more security bugs are discovered and addressed.[154] Without adequate legal protections built into VDPs, there will be little incentive for ethical hackers to collaborate with organizations, including companies behind the world's most widely used products and services. While the U.S. government makes up only a portion of the VDP industry, if there is a chilling effect on security research due to inadequate legal protections, the number of eyes available to help solve significant cyber risks, and challenges within the government will decrease as well. The DOJ Framework is a first step to improve VDP practices across host organizations, and the recommendations outlined in this Note improve the existing system by suggesting methods to increase use of the DOJ Framework. While the DOJ may not have binding authority through the VDP guidelines laid out in its framework, creating a direct line of communication with stakeholders, updating potentially outdated recommendations, and looking to the DHS' binding Directive and government agency VDPs as a model has the potential to bridge the gap created by the DOJ Framework's voluntary self-governance model and the current issues faced in the VDP world.

153. Maillart et al., *supra* note 24, at 82.
154. *Id.*