Federal Trade Commission Public Comment on NTIA Safety Working Group's "Coordinated Vulnerability Disclosure 'Early Stage' Template"

Thank you for the opportunity to comment on the NTIA Safety Working Group's "Coordinated Vulnerability Disclosure 'Early Stage' Template."[1] Coordinated vulnerability disclosure refers to a company's defined policies and procedures for receiving and responding to information about vulnerabilities in its products and services from security researchers and other stakeholders. It can help create common expectations with respect to processes for vulnerability disclosure, communication, and remediation. As software-based products spread throughout the economy, it is important that all stakeholders work together to ensure the security and safety of these products.

The Commission would like to thank NTIA for its work in promoting coordinated vulnerability disclosure through the multistakeholder process. Through its enforcement actions and business education efforts, the FTC has encouraged companies to have adequate processes to receive and address vulnerability reports as a part of a comprehensive plan to ensure the security of software and consumer devices throughout the product lifecycle. Consistent with this approach, the NTIA Safety Working Group's "Coordinated Vulnerability Disclosure 'Early Stage' Template" provides businesses with an adaptable model for implementing a vulnerability disclosure policy appropriately tailored to the company's size and resources, and offers valuable guidance on the critical questions companies must ask when developing such policies and procedures. The Commission appreciates the efforts of the security researchers, software companies, security companies, academics, and civil society advocates that participated in the NTIA's year-long multistakeholder process on this important topic.

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. The FTC has undertaken substantial efforts for well over a decade to promote data security in the private sector through civil law enforcement, business outreach and consumer education, policy initiatives, and recommendations to Congress regarding data security legislation. The FTC relies on Section 5 of the FTC Act as the primary enforcement tool to prevent deceptive and unfair business practices in the area of data security. The Commission also enforces requirements in laws applicable to consumer reports, children's information, and financial institutions that relate to data security. Since 2001, the FTC has obtained settlements in some 60 cases against companies the FTC alleges failed to provide reasonable protections for consumers' personal information. From the outset, the FTC has recognized that there is no such thing as perfect security, and that security is a continuing process of detecting risks and adjusting one's security program and defenses.

To that end, the FTC has recommended that, in conjunction with implementing secure coding standards, vulnerability testing, and other secure development practices, companies should communicate and coordinate with the security research community as part of a

[1] NTIA SAFETY WORKING GROUP, "EARLY STAGE" COORDINATED VULNERABILITY DISCLOSURE TEMPLATE VERSION 1.1 (2016) [hereinafter DISCLOSURE TEMPLATE], https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf.

continuous process of detecting and remediating software vulnerabilities. Given the complex nature of software, security-related bugs are inevitable, and the research community represents a critical tool in defending against the exploit of such vulnerabilities. Studies have found that the adoption of vulnerability disclosure policies represents a cost-effective and efficient method of identifying and addressing vulnerabilities.[2] The Commission's work in this area (as detailed further below), the NTIA multistakeholder process, and the work of other federal agencies such as the Food and Drug Administration[3] and the Library of Congress[4] show the importance of coordinated vulnerability disclosure in helping companies address security vulnerabilities that affect not only their own products and customers but also the Internet ecosystem as a whole.

The Commission first addressed the importance of coordinated vulnerability disclosure in an enforcement context through its case against mobile device manufacturer HTC America, Inc. ("HTC") in February 2013. The Commission's complaint charged that, among other things, HTC failed to "implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics, or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents."[5] In its settlement with the Commission, HTC agreed to establish a comprehensive security program that included processes for the "review, assessment, and response to third-party security vulnerability reports."[6] In a business education piece published at that time, Commission staff highlighted the important role that vulnerability reports play in ensuring product security, and recommended that businesses implement reasonable vulnerability disclosure processes to facilitate communication with the research community.[7]

---

[2] *See* Matthew Finifter et al., *An Empirical Study of Vulnerability Rewards Programs*, 22ND USENIX SECURITY SYMPOSIUM 273 (2013), https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf.

[3] *See* Suzanne B. Schwartz, *Managing Medical Device Cybersecurity in the Postmarket: At the Crossroads of Cyber-safety and Advancing Technology*, FDA VOICE (Dec. 27, 2016), http://blogs.fda.gov/fdavoice/index.php/2016/12/managing-medical-device-cybersecurity-in-the-postmarket-at-the-crossroads-of-cyber-safety-and-advancing-technology/ (recommending that medical device manufacturers "establish a process for working with cybersecurity researchers and other stakeholders to receive information about potential vulnerabilities (known as a 'coordinated vulnerability disclosure policy')").

[4] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies 80 Fed. Reg. 65944 (October 28, 2015) (creating exemption from liability under the Digital Millennium Copyright Act for "good-faith security research"); *see also* Aaron Alva, *DMCA security research exemption for consumer devices*, TECH@FTC (Oct. 28, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices (discussing the exemption).

[5] HTC America, Inc., No. 122 3049 (F.T.C. June 25, 2013) (complaint), https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf. Acting Chairman Ohlhausen was recused from this matter.

[6] HTC America, Inc., No. 122 3049 (F.T.C. June 25, 2013) (decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf. Acting Chairman Ohlhausen was recused from this matter.

[7] Lesley Fair, *Batten down the patches: Six points to take from the FTC settlement with HTC*, FED. TRADE COMM'N: BUSINESS BLOG (Feb. 27, 2013, 11:49 AM), https://www.ftc.gov/news-events/blogs/business-blog/2013/02/batten-down-patches-six-points-take-ftc-settlement-htc ("**Listen up!** The tech world is full of researchers, academics, and

Since the HTC matter, the Commission has obtained settlements in additional product security cases that include similar consent order provisions requiring the establishment of vulnerability disclosure policies and procedures, such as TRENDnet, Inc.,[8] Fandango LLC,[9] Credit Karma, Inc.,[10] and ASUSTeK Computer, Inc.[11]

The Commission has also addressed this issue in its data security guidance,[12] its policy reports,[13] and through its business education campaigns. For example, the Commission's September 2015 Start with Security business education conference featured a panel of vulnerability disclosure experts providing practical advice on how companies can best respond to vulnerability reports.[14] The panel included an in-depth discussion of the processes set forth in

---

savvy users who are constantly testing and tinkering with your products. They're often the canaries in the coal mine that spot potential problems before companies do. So it's wise to keep the lines of communication open. The FTC's complaint charged that HTC failed to implement a process for receiving and addressing security vulnerability reports from researchers, academics, or members of the public. Had HTC been listening, the FTC says it could have moved faster to correct vulnerabilities. There's no one-size-fits-all best way to keep the channels open, but it should be part of any effective comprehensive security program").

[8] TRENDnet, Inc., No. 122 3090 (F.T.C. Jan. 16, 2014) (decision and order), https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

[9] Fandango, LLC, No. 132 3089 (F.T.C. Aug. 13, 2014) (decision and order), https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf.

[10] Credit Karma, Inc., a corporation, No. 132 3091 (F.T.C. Aug. 13, 2014) (decision and order), https://www.ftc.gov/system/files/documents/cases/1408creditkarmado.pdf.

[11] ASUSTeK Computer Inc., No. 142 356 (F.T.C. July 18, 2016) (decision and order), https://www.ftc.gov/system/files/documents/cases/1607asustekdo.pdf.

[12] *See, e.g.*, FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (recommending that companies "have an effective process in place to receive and address security vulnerability reports. Consider a clearly publicized and effective channel (for example, a dedicated email address like security(@)yourcompany.com) for receiving reports and flagging them for your security staff."); *see also* FED. TRADE COMM'N, MOBILE APP DEVELOPERS: START WITH SECURITY (2013), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security (recommending that mobile app developers "check your inbox, too. User feedback can help you spot and fix security vulnerabilities. When they discover vulnerabilities, researchers often try to resolve the issue with developers before publishing their findings. It's best to be part of that discussion early on.").

[13] *See* FED. TRADE COMM'N, FTC STAFF REPORT: INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD 31-32 (2015) [hereinafter INTERNET OF THINGS REPORT], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (encouraging Internet of Things manufacturers to "monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.").

[14] *See* Agenda, Fed. Trade Comm'n, Start with Security – San Francisco (Sept. 9, 2015), https://www.ftc.gov/news-events/events-calendar/2015/09/start-security-san-francisco ("Panel 3: Bugs and Bounties: Vulnerability Disclosure and Response. How should startups respond when hackers come calling? From the basics of bug triage to running a full-scale bounty, this panel will examine how startups can successfully manage, address, and — perhaps most importantly — learn from vulnerability reports, harnessing the work of the security community to improve their

ISO/IEC Standards 29147 and 30111,[15] and covered how companies can appropriately scope vulnerability disclosure programs, triage and address vulnerability submissions, and incentivize vulnerability reporting.

In addition, when Commission staff solicits research relating to security vulnerabilities, staff has emphasized coordinated vulnerability disclosure. For example, the Commission has held two "PrivacyCon" conferences as a forum for discussion of research in the data security and privacy fields. In seeking research submissions for the PrivacyCon events, the FTC requires researchers to disclose any previously unknown security or privacy vulnerability in a specific product or service to the company that developed the product or service, and to provide the company with time to resolve the issue.[16]

As the NTIA Awareness and Adoption Group's "Vulnerability Disclosure Attitudes and Action" report found, the vast majority of researchers engage in coordinated vulnerability disclosure when given the opportunity, and typically resort to public disclosure only when they are unable to communicate effectively with affected companies.[17] Given this finding, the "Coordinated Vulnerability Disclosure 'Early Stage' Template" represents an important additional resource for companies that are considering the adoption of vulnerability disclosure policies and procedures as part of a comprehensive data security program. Both companies and researchers should deal with one another fairly and transparently during the vulnerability reporting process. As a supplement to existing standards, the draft template provides companies with model language that could be a useful asset for companies seeking to draft a public-facing vulnerability disclosure policy that helps forge common expectations with researchers regarding vulnerability handling timelines and processes.

---

secure development lifecycle."). The Commission's Start with Security business education initiative included both a new Guide for Business, *see supra* note 11, as well as a series of conferences across the country that brought together data security experts to provide advice on a wide-range of security-related topics.

[15] ISO/IEC 29147, Vulnerability Disclosure (2014), is a standard that details the methods a company should use to address issues related to vulnerability disclosure. It is available at http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170 and at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html. ISO/IEC 30111, Vulnerability Handling Processes (2013), is a standard that provides guidelines for how to process and resolve vulnerabilities in a product or online service. It is available at http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231. The "Coordinated Vulnerability Disclosure 'Early Stage' Template" also references the ISO/IEC standards. *See* DISCLOSURE TEMPLATE, *supra* note 1, at 4.

[16] *See* Fed. Trade Comm'n, PrivacyCon: Call for Presentations (2016), https://www.ftc.gov/privacycon-call-for-presentations ("Research exposing a previously unknown security or privacy vulnerability in a specific product or service will only be accepted if it has been responsibly disclosed to the affected entity and that entity has been given time to resolve the issue. Such Requests must be submitted only through the Accellion secure file transfer system described below and must be accompanied by: (1) a request for confidential treatment of research, and (2) a statement describing how you responsibly disclosed the vulnerability to the entity responsible for the affected product or service.").

[17] *See* NTIA AWARENESS AND ADOPTION GROUP, VULNERABILITY DISCLOSURE ATTITUDES AND ACTIONS 2 (2016), https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

FTC staff notes that the template as currently drafted is directed towards companies in safety-critical industries, such as the automobile and medical device industries. While the FTC has recognized that companies in safety-critical industries should take more robust measures to ensure the security of their software,[18] FTC staff believes that the template could be a useful tool for any company providing software-based products and services to consumers. Indeed, the draft template's "Executive Summary" notes that the "lessons are easily adaptable by any organization that builds or maintains its own software or systems."[19] To that end, FTC staff recommends that the draft template's introduction be revised to make clear that its recommendations may be more broadly applicable. In particular, companies that provide Internet-connected products[20] or collect sensitive consumer information should consider implementing a vulnerability disclosure policy and related processes.

Thank you again to NTIA and all of the stakeholders that contributed to this process.

---

[18] *See* INTERNET OF THINGS REPORT, *supra* note 13, at 33 (calling for more robust security for devices that collect sensitive information, present physical security or safety risks, or if breached could enable intruders to access other connected devices or networks).

[19] DISCLOSURE TEMPLATE, *supra* note 1, at 1.

[20] *See, e.g.*, Alert, U.S. CERT, Heightened DDoS Threat Posed by Mirai and Other Botnets, (Nov. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA16-288A. The FTC recently announced a prize competition that challenges the public to create a technical solution that consumers can deploy to guard against security vulnerabilities in software on Internet of Things devices in their homes. *See* Press Release, Fed. Trade Comm'n, FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices: Contestants will compete for top prize of $25,000 for best technical solution (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security.