December 12, 2023

Recommendations to encourage adoption of coordinated vulnerability disclosure under the National Cybersecurity Strategy

The National Cybersecurity Strategy announced the White House's intention to "encourage coordinated vulnerability disclosure across all technology types and sectors" in order to further incentivize the adoption of secure software development practices."[1] The National Cybersecurity Strategy Implementation Plan reiterated the goal to "build domestic and international support for an expectation of coordinated vulnerability disclosure among public and private entities, across all technology types and sectors."[2] However, the Implementation Plan included very limited action items to achieve this.

Below, the Hacking Policy Council (HPC) shares feedback and recommendations to help advance the Strategy's objective of encouraging cross-sector adoption of coordinated vulnerability disclosure.

1) **Community of interest:** The Implementation Plan proposes that the Cybersecurity and Infrastructure Security Agency (CISA) create an international community of practice to "build global awareness and capacity around coordinated vulnerability disclosure." HPC is concerned that this is a very narrow goal and is redundant of existing efforts with the public and private sectors, particularly the Forum of Incident Response and Security Teams (FIRST) Community, in which HPC members presently participate. Asking organizations to join yet another working group risks requiring additional resource expenditure for little additional impact. Rather than creating a new community of interest, HPC recommends establishing a subgroup of FIRST, the National Cybersecurity Center of Excellence (NCCoE), or other existing efforts. HPC also urges CISA to work collaboratively with the Department of State on international coordination in connection with this effort.

2) **Regulatory updates:** HPC recommends federal agencies incorporate vulnerability disclosure and handling programs into cybersecurity and privacy regulatory updates across all sectors, in alignment with best practices. For example, the Implementation Plan prioritizes establishing cybersecurity requirements across critical infrastructure sectors, and

[1] White House, National Cybersecurity Strategy, Objective 3.3, Mar. 2023, pg. 21, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[2] White House, National Cybersecurity Strategy Implementation Plan, Initiative 3.3.3, pg. 31, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

CISA has included vulnerability disclosure in the Cross-Sector Cybersecurity Performance Goals meant to guide baseline security practices across critical infrastructure sectors.[3] However, not even recent critical infrastructure cybersecurity regulatory updates include requirements to adopt vulnerability disclosure programs.[4] As regulations across all sectors are revised, and as new regulations are considered, vulnerability disclosure and handling programs in alignment with internationally recognized standards such as ISO/IEC 29147 and 30111 should be established as a component of organizational security requirements.

3) **Sanctions clarification:** The Administration should work with the Office of Foreign Assets Control (OFAC) to issue regulatory guidance regarding coordinated vulnerability disclosure processes and sanctions. This guidance should clarify that it is not a sanctioned event for organizations to receive a cybersecurity vulnerability disclosure from individuals in comprehensively sanctioned countries and regions, and for the organization to ask follow-up questions regarding that vulnerability, when no payment or service is provided to the individual making the disclosure. Separately, we also suggest evaluating sanctions and receipt of cybersecurity vulnerability disclosure from individuals with a connection to entities on the Specially Designated Nationals (SDN) list (for example, an individual who was employed by a company listed on the SDN, but is not themselves individually listed). Such policies could be better harmonized with the Bureau of Industry and Security Cyber Rule, which authorizes exports involving vulnerability disclosures.[5]

4) **Contractor requirements:** As a component of Federal Acquisition Regulation updates, federal civilian and defense contractors should be required to adopt vulnerability disclosure and handling processes in alignment with internationally recognized standards. Contractors should decline to bring lawsuits for acts of good faith security research conducted in alignment with best practices.

5) **Standards and guidance:** Vulnerability disclosure and handling processes should be explicitly included as part of agency guidance, NIST security standards, and best practice documents detailing components of basic security programs, with reference to internationally recognized standards. This should include agency guidance on expectations for reasonable security programs.[6] The Administration should also work with public and private sector standards bodies to encourage inclusion of vulnerability disclosure and handling processes.

[3] CISA, Cross-Sector Cybersecurity Performance Goals, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals (last accessed Nov. 21, 2023).

[4] See, for example, Transportation Security Administration, SD 1580_1582-2022-01A - Rail Cybersecurity Mitigation Actions and Testing, Oct. 23, 2023, https://www.tsa.gov/sites/default/files/sd-1580_1582-2022-01a-rail-cybersecurity-mitigation-actions-and-testing.pdf.

[5] 15 CFR 740.22.

[6] See, for example, Federal Trade Commission, FTC Safeguards Rule: What Your Business Needs to Know, May 2022, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.

6) **Trade agreements:** The Administration should include coordinated vulnerability disclosure into digital trade negotiations. Free trade agreements should encourage enterprises and government bodies to adopt coordinated vulnerability disclosure and handling processes aligned with internationally recognized standards.[7] Such negotiations are especially needed as some global governments do not follow internationally recognized coordinated vulnerability disclosure practices, creating a risk of further global adoption of this model.

7) **State laws:** HPC recommends encouraging states and municipalities to require vulnerability disclosure programs for their agencies, in alignment with best practices and industry norms, as federal agencies are required to do under CISA Binding Operational Directive 20-01.[8] HPC also recommends working with state Attorneys General to adopt policies to decline charging individuals for acts of good faith security research, consistent with the Computer Fraud and Abuse Act charging policy adopted by the U.S. Department of Justice.[9]

* * *

[7] Cybersecurity Vulnerability Disclosure in Trade Agreements, Rapid7, Mar. 24, 2020, https://www.rapid7.com/blog/post/2020/03/24/cybersecurity-vulnerability-disclosure-in-trade-agreements.

[8] See, for example, New York City, Office of Technology and innovation, NYC Cyber Command Establishes New York City's First Vulnerability Disclosure Program, Oct. 31, 2023, https://www.nyc.gov/content/oti/pages/press-releases/nyc-cyber-command-establishes-new-york-city%E2%80%99s-first-vulnerability-disclosure-program.

[9] Hacking Policy Council, Position Statement on State Charging Policies for Security Researchers, Aug. 8, 2023, https://assets-global.website-files.com/62713397a014368302d4ddf5/64d3d1e780453a690d637186_HPC%20statement%20on%20state%20charging%20policy%20reform%20-%20August%202023.pdf.