ASPEN POLICY ACADEMY
aspen institute

CASE STUDY: December 2024

IMPACT CASE STUDY

Advancing Cybersecurity On a National Level

The Aspen Institute's Policy Academy turns professionals into policy advocates. We offer innovative training programs to equip leaders across sectors – from tech to climate, science to social impact – with the practical policy skills to craft solutions for society's most pressing challenges. Based in the Bay Area, the Policy Academy is the first comprehensive nonpartisan and non-university training program in the United States offering a step-by-step process to learn practical strategies for policymaking. The Academy's predecessor, the Aspen Tech Policy Hub, has helped more than 500 alumni and staff gain government experience and seek policy impact.

EXECUTIVE SUMMARY

In 2020-2021, Aspen Policy Academy alumni Anil Dewan and Alexander "RoRo" Romero led the effort to expand the scope of the Department of Defense (DoD)'s Vulnerability Disclosure Program (VDP). This critical cybersecurity program provides legal safe harbor to researchers who find and report vulnerabilities in DoD information systems using established protocols. These reports enable the DoD to quickly validate and remediate the vulnerabilities while ensuring that the researchers are not prosecuted for their service. The original VDP only applied to public-facing DoD websites. Using skills they learned at the Aspen Policy Academy, Anil and RoRo successfully expanded the policy to apply to all publicly accessible DoD information systems. This policy change allowed for more vulnerabilities to be reported and increased security of DoD systems and, as a result, the security of our nation.

BACKGROUND

In 2016, the DoD challenged researchers around the world to find and report vulnerabilities in DoD systems, via a hack-a-thon. RoRo was part of the original team from Defense Digital Service (DDS) that spearheaded this initiative. The success of the

aspen institute

hack-a-thon led the DoD to establish the VDP to allow researchers to continue to find and report vulnerabilities with legal protections in place. The original VDP applied to "Any public-facing website owned, operated, or controlled by DoD, including web applications hosted on those sites." The DoD also expanded its own ethical hacking program called "Hack the Pentagon" by creating specific bug bounty events with hackers to find vulnerabilities in these programs. RoRo and Anil were asked to lead this program in 2019.

The success of Hack the Pentagon and the VDP led to the insight that additional DoD information systems needed to be made available because "public-facing websites" left many critical systems out of scope and therefore potentially vulnerable. Researchers were finding vulnerabilities in emails, mobile apps, databases, and other critical systems that they could not safely report without fear of prosecution. RoRo and Anil knew the VDP scope needed to be expanded and took on the challenge to drive the policy change. Their fellowships at the Academy equipped them to both understand the government policymaking process and work collaboratively with stakeholders across the DoD to create the major revision to the policy.

IMPACT

To ensure the policy was approved quickly, the team narrowly focused on expanding the scope of information systems covered by the VDP. RoRo and Anil changed 16 words to the scope of the VDP, proposing that the policy apply to "Any publicly accessible information system, web property, or data owned, operated, or controlled by the DoD." By focusing on only 16 words, they were able to limit potential areas of disagreement or concern from stakeholders and obtain approval from all required officials, getting the change signed by then-Acting Secretary of Defense David Norquist.

Thanks to the 16-word change (and a few more words added by the legal team) the VDP was expanded to include all publicly accessible DoD information systems. This expansion had an immediate impact: During the updated VDP's 3-month trial period, researchers who had not reported known vulnerabilities were able to safely submit them to the DoD. RoRo and Anil's work also inspired the adoption of a VDP across the entire defense industrial base, including companies and their subcontractors who work with the DoD. Between the broader policy and its broader adoption, the growth in vulnerability reporting has been ongoing, with more vulnerabilities being reported and corrected every day. This change has increased the security of DoD systems and, as a result, the national security of the United States. As of March 2023, the DoD VDP program had received more than 53,000 vulnerability reports, underscoring its impact in improving the security of our nation.