IMPACT CASE STUDY

Leading Cybersecurity Impact Across Sectors

CASE STUDY: JUNE 2025

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

Daniel Bardenstein joined the Aspen Policy Academy as a Tech Policy Fellow in 2021 to hone his policy skills and figure out how to get into government from the private sector. The fellowship helped Daniel translate his interests in medical cybersecurity into project work and policy skills, which were invaluable in his later role as the Chief of Technology Strategy at the US Cybersecurity and Infrastructure Security Agency (CISA).

BACKGROUND

Before his time with the Academy, Daniel was a cybersecurity lead for the development of the COVID vaccine. He uncovered a significant gap in the healthcare and medical supply chain as healthcare organizations have become increasingly vulnerable to ransomware and cyberattacks. Daniel joined the fellowship program both because he had an eye toward joining government, and because he had a 'policy itch' he wanted to scratch. He was particularly interested in strengthening cybersecurity measures for medical devices and providing the technical architecture for manufacturers and hospitals to secure devices without compromising their functionality.

As part of his fellowship, Daniel created the policy project "'Smart' but Insecure: Improving Medical Device Cybersecurity" to address how the Food and Drug Administration (FDA) can simplify the process hospitals use to secure medical devices. In his project, Daniel advised the FDA to develop a minimum baseline of cybersecurity requirements for medical device manufacturers, and proposed a novel software concept, the 'Device Query Interface', which addressed the risk of medical devices failing while trying to perform routine security checks and operations.

> *"The program gave me the understanding of nuances of government roles and responsibilities, so when I had the opportunity to provide input, I felt better able to do so and was more impactful than I otherwise would have been."*
>
> Daniel Bardenstein

IMPACT

Daniel succeeded in pitching his proposal to a number of stakeholders, including the FDA, the Health Care Sector Coordinating Council, and the former CTO of the White House. Daniel discovered that at the time his project was published, the FDA didn't have the authority to establish a minimum cybersecurity baseline. Congress has since granted the FDA specific authority to update device cybersecurity measures.

Daniel then went on to achieve his goal of joining government, becoming the Chief of Technology Strategy at CISA. Coincidentally, his portfolio included establishing minimum cybersecurity baselines. Relying on the lessons he learned at the Academy and through his final project, Daniel led the development of CISA's cross-sector cybersecurity performance goals. In his CISA role, he also regularly contributed to policy documents such as executive orders and the National Cyber Strategy.

Though he has since left government, Daniel continues to have policy impact as the CTO and co-founder of the cybersecurity company Manifest. For instance, Daniel recently won a 'Cyber Shark Tank' competition which led to him working with the Senate Intelligence Committee on a bill about supply chain security.