Written Testimony of Jack Cable
CEO & Co-Founder
Corridor

Before the U.S. House Committee on Homeland Security

Hearing on
"Innovation Nation: Leveraging Technology to
Secure Cyberspace and Streamline Compliance"

May 28, 2025

Chairman Green, Ranking Member Thompson, Chairman Garbarino, and Ranking Member Swalwell, it is my honor to testify here today.

My name is Jack Cable. I am the CEO and Co-Founder of Corridor, a company using AI to help make secure by design software a reality. Our platform can understand the security model of a codebase, refactor unsafe patterns, and add guardrails around AI coding assistants.

This is a deeply personal topic for me. We're here at Stanford, my alma mater, where I studied computer science. Throughout my career, I've prided myself on finding innovative solutions to the hardest problems in cybersecurity. As a self-taught ethical hacker, I've worked in the private sector, academia, and government to advance the state of software security. Most recently, I helped lead CISA's Secure by Design and open source software security initiatives, including creating the Secure by Design pledge, where hundreds of companies have committed to demonstrating their progress in securing their software.

I've seen firsthand how insecure software can jeopardize our public safety, particularly as both nation-state actors and cybercriminals seek to compromise our nation's critical infrastructure. And I've seen how technological advancements like AI can both help improve our collective state of security and magnify existing vulnerabilities.

As this Committee has highlighted, state-sponsored hackers from the People's Republic of China are currently burrowed within our critical infrastructure. Should China invade Taiwan, they stand to conduct destructive cyberattacks on our power grids, water systems, telecom providers, and more.

But these attacks are not inevitable, nor unpreventable. The vast majority of cyberattacks take advantage of either a preventable software vulnerability or an insecure default configuration.[1] This could be as simple as a temporary default password intended to be changed right away that sits unchanged. Rather than placing the burden on end-users to take care of these problems, software manufacturers can build their products to be secure by design and thus raise costs on our adversaries. Secure by design software is our best hope to defend against PRC cyber threats. The time to act is now.

The Promises and Perils of AI

There is a revolution happening in software development right now. It's now possible to build a website with just a one-sentence prompt. The overwhelming majority of developers are now using AI coding assistants,[2] enabling them to ship software faster than ever before.

---

[1] https://hbr.org/2024/04/preventing-ransomware-attacks-at-scale
[2] https://github.blog/news-insights/research/survey-ai-wave-grows/

AI coding models can introduce the same vulnerabilities that we've known about for decades. Studies have found that even the best models write vulnerable code about 30-40% of the time.[3,4] It's only a matter of time until AI coding assistants introduce a severe vulnerability in critical software that is exploited.

At Corridor, we're using AI to secure software without slowing down development. With our technology, we can add guardrails to AI assistants, preventing them from introducing vulnerable code in the first place. Companies adopting AI coding assistants must take a proactive stance and enact guardrails now.

We also need to make sure that current and future software developers understand the basics of security. Alarmingly, none of the top 20 degree programs in computer science require a course in security to graduate. We wouldn't let civil engineers graduate without understanding how to build safe bridges. So why do we allow software engineers to get a degree without knowing how to build secure systems?

Secure by Demand

At CISA, we were often asked whether secure by design would stifle innovation. As someone who's building my own company today, I can say that there doesn't have to be a tradeoff between security and innovation. The security of a software system is a property of the overall quality of the software. The same design decisions that make our systems more resilient and secure by default also lead to higher quality code that costs less to maintain. The fact that over 300 companies voluntarily committed last year to CISA's Secure by Design Pledge is another sign that security and innovation can go hand-in-hand.

By working together, we can accelerate the pace of adoption of secure by design practices – and this takes everyone, including software manufacturers and their customers. Last month, the Chief Information Security Officer of JP Morgan Chase published a letter saying that third-party software suppliers are enabling cyberattacks, and urging them to prioritize security.[5]

At CISA, we called this "Secure by Demand". All software customers can help to raise the bar for the product security of their vendors.

The U.S. government should play a key role by doing away with check-the-box, compliance-oriented procurement processes and starting to measure actual product security practices. Today, far too many requirements focus on the enterprise security practices of the

[3] https://baxbench.com/
[4] https://dl.acm.org/doi/full/10.1145/3610721
[5] https://www.jpmorgan.com/technology/technology-blog/open-letter-to-our-suppliers

company building the software, rather than the actual security of the product itself. This is akin to testing that a factory has locked its doors, but not evaluating the products that the factory is producing.

CISA's Secure Software Development Self-Attestation form is a good starting point. I encourage Congress and the Administration to expand on this to include more outcomes-based product security measures, such as from CISA's pledge and the Product Security Bad Practices list, to further incentivize software manufacturers to build their products with security from the start.

CVEs and Vulnerability Disclosure

I recently published a piece with former CISA Director Jen Easterly advocating for Congress to strengthen the security research ecosystem in the United States.[6] Security researchers like myself play a crucial role in discovering and reporting vulnerabilities before our adversaries can.

The PRC has enacted laws to require security researchers to report vulnerabilities to the Chinese government before disclosing to vendors. We must counteract this with an open and transparent security research ecosystem in the U.S.

While we've made progress in recent years, anti-hacking laws like the Computer Fraud and Abuse Act (CFAA) still have a chilling effect on good-faith security research. Congress should reform the CFAA – and associated laws such as Section 1201 of the Digital Millennium Copyright Act (DMCA) – to exempt good-faith security research. The Department of Justice has worked over the last decade to demonstrate an understanding in the value of good-faith security research and to discourage legal action against ethical hackers. Nonetheless, as with other laws that protect unintended targets of legal action, the security community should not and cannot rely solely on prosecutorial discretion to protect good-faith security research from legal retaliation.

Additionally, the Common Vulnerabilities and Exposures (CVE) program is an essential resource for tracking vulnerabilities and their root causes. We must ensure that this critical program continues and that all companies issue complete, accurate, and timely CVE records for their vulnerabilities.

Congress should codify, under CISA, the CVE program's essential mission as a national record of security flaws, and normalize vulnerability disclosure by eliminating barriers to security research.

[6] https://www.lawfaremedia.org/article/advancing-secure-by-design-through-security-research

Conclusion

In conclusion, we must act now to secure the threats of today, and those that will come tomorrow. By addressing the risks posed by AI, raising the bar through federal procurement, and fostering a healthy security research ecosystem, we can fundamentally secure software and raise costs on our adversaries.

Finally, I would be remiss not to recognize the exodus of technical talent that has occurred at CISA over the last several months. I have personally seen how CISA has lost its very best. In the face of increasing threats, we can't undermine the capacity of America's Cyber Defense Agency and its ability to attract and retain the best technical talent. This only makes us less secure as a nation.

Thank you. I look forward to your questions.