Questions for the Record
U.S. Senate Select Committee on Intelligence
Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center
Open Session
September 21, 2022

Robert Sheldon
Director, Public Policy & Strategy

[From Senator Feinstein]

The U.S. Counterintelligence Enterprise

1. **Which legal responsibilities should non-IC entities—including U.S. government agencies, academic institutions, and private sector companies—have to protect their intellectual property, research, technologies, and data with national security implications?**

There is no single, uniform data protection scheme for national-security relevant information. Laws, regulations, contracts, and customer commitments or expectations can each apply particular requirements, depending on the context. This system does create the potential for gaps or overlaps. However, a singular approach to protecting national-security relevant information may also carry risks. These include impacts to the pace of cross-functional research, research in areas with dual-use implications, and innovation generally. Where the U.S. government issues specific guidance, such as threat advisories, to sectors or organizations then it is important to advise on how to mitigate such threats and to empower them with the appropriate tools to do so where they may not exist.

2. **Which incentives and resources could Congress provide to help non-Intelligence Community entities better protect their intellectual property, research, technologies, and data from foreign adversaries?**

Two lines of effort could help organizations become better informed about threats and take steps to stop them. (A) The U.S. national security enterprise should more clearly communicate areas of research/technology with perceived national security implications. Proactive disclosures about emerging intelligence collection requirements from foreign adversaries would help inform the threat model used by entities working in those areas. (B) From a cybersecurity standpoint, targeted efforts to increase defenses by small- and medium-sized entities could be impactful. To this end, as noted in my testimony, Congress could take steps to increase national incident response capacity and explore tax-mechanisms to promote and enhance adoption of comprehensive cybersecurity solutions.

3. **What are the biggest challenges private sector entities face in confronting foreign adversarial intelligence collection and economic espionage?**

While private sector entities face an array of threats that range from problematic investors to malicious insiders, cybersecurity remains the central challenge. Even entities that follow all current, applicable cybersecurity controls and best practices will be breached periodically by capable adversaries. To successfully face these challenges, organizations must continuously improve their cybersecurity posture, adopt zero trust principles, and proactively hunt threats within their networks. Organizations should strongly consider leveraging managed security services providers to operate with the speed necessary to defeat threats.

4. **Given the generally lawful nature of foreign acquisition of U.S. technology, does Congress need to consider additional updates to the Committee on Foreign Investment in the United States (CFIUS) to address remaining loopholes?**

While my co-panelists are better situated to address CFIUS-related questions, I'll make two minor observations. First, given macroeconomic conditions, it is reasonable to assume an increased rate of M&A activity across the technology and startup ecosystem over the coming years. Second, in addition to broad transaction-related risks, CrowdStrike has observed threat actors specifically targeting entities engaged in the M&A process.

5. **How can the U.S. government best strike a balance between protecting national security and preserving a culture of international collaboration, free enterprise, and open research?**

While my co-panelists are better situated to address this question, I note that a key step is the potential to exacerbate potential tensions between these aims with insufficiently nuanced policy. Continuing the Committee's approach to engaging stakeholders from different backgrounds and with different perspectives is key, as is broadening outreach to different parts of industry.

6. **To what extent should the State Department vet foreign students, professors, or employees from a counterintelligence perspective?**

Whether an individual is from a foreign country may not warrant additional scrutiny on its own. Instead, to the extent that additional vetting is required, it should be risk-informed, consistent, fair, and account for differences between these stakeholder groups. Like with positions of trust, a totality of circumstances may warrant additional scrutiny. For example, a student from one country studying at a liberal arts university may merit a different process than an employee from a country with a targeted espionage apparatus working in a lab supported by U.S. government funding for defense-relevant research.

7. **How can the U.S. government in general and the Intelligence Community in particular better communicate the foreign intelligence threat to the American public, private sector companies, and academic institutions?**

As noted above (in Answer 2(A)), the Government and Intelligence Community can help identify new targets or trends in foreign intelligence collection priorities. In some instances, broad communications about these developments may be appropriate. In other instances, the government can provide more clarity–and reach scale–by working through trusted entities with more expansive commercial relationships. To these ends, models like CISA's Joint Cyber Defense Collaborate (JCDC) merit continued experimentation and investment.

8. **How can the U.S. government in general and the Intelligence Community in particular partner with non-Intelligence Community entities to prevent foreign intelligence penetration and exploitation?**

As noted above, from an industry engagement perspective, policymakers should explore broadening access to cybersecurity capabilities and increase incident response capacity (Answer 2) and explore greater use of JCDC and similar mechanisms (Answer 7).

Further, the U.S. should use all mechanisms at its disposal, including industry engagement where appropriate and additive, to degrade threat actors' ability to effectuate malicious cyber activity. This includes cooperative efforts to directly target malicious infrastructure.

9. **CrowdStrike is a recognized leader in cybersecurity.**

    a. **From your perspective, what role should commercial providers play in defending academic institutions and private sector entities from foreign intelligence entity cyber attacks?**

The private sector is on the "front lines" combating cyber threats. Government entities can and should help communicate new threats and coordinate response efforts, as well as reduce the overall threat environment (e.g., as described in Answer 8). But commercial providers perform the actual defense, and in virtually all cases also perform response and remediation in response to incidents. From a roles and missions standpoint, this division of labor is appropriate given each entities' respective authorities, missions, resources, and capabilities. The central policy questions relate to how each entity can perform their missions better, with more efficiency, and at greater scale.

    b. **How can commercial cybersecurity providers such as CrowdStrike better partner with the U.S. government to defend non-Intelligence Community entities from foreign cyber attacks?**

The U.S. government, particularly the nation's lead federal agency for the protection of critical infrastructure, the Cybersecurity and Infrastructure Security Agency (CISA) does not have the cyber incident response capacity needed to respond to broad-based, concurrent significant cyber incidents impacting critical infrastructure entities or the federal government.

As a community, we should undertake a more serious conversation about expanding national Incident Response (IR) capacity. IR demand is incredibly elastic, and IR supply is relatively fixed. A program that retained skilled providers in advance for use during significant cyber incidents could expand the cybersecurity workforce and strengthen national resilience. Such a program would ensure skilled providers are standing ready to offer assistance within a stipulated time frame, and under other terms outlined in a Service Level Agreement (SLA).

Eligibility for benefits under such a program would likely be based on need or vulnerability (e.g., for small businesses), and/or on criticality (e.g, entities with a national security nexus or critical infrastructure entities with systemic importance), in accordance with CISA's judgment.

c. What role, if any, should U.S. government entities such as CYBERCOM play in defending non-U.S. government entities from foreign cyber attacks?

Please see Answer 8.

d. What statutory or policy changes, if any, are necessary to clarify and strengthen the relationship between commercial cybersecurity providers and the U.S. government?

The current balance of responsibilities between commercial cybersecurity providers and various government agencies is the result of several decades of iteration, experimentation, stress-tests, case law, etc. Like other complex policy areas, outcomes are far from perfect. But the fundamental roles and missions of each sector (described in Answer 9a) are sound. Each sector should continue to develop its capacity to meet evolving threats (see Answer 2), and each sector should work together in a more integrated way (see Answer 7).

###