Testimony Of

Drew Bagley
Vice President & Counsel for Privacy and Cyber Policy
CrowdStrike

Before

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective"

March 23, 2023

Chairman Garbarino, Ranking Member Swalwell, members of the subcommittee, thank you for the opportunity to testify today. We are at a pivotal moment in the cybersecurity challenges posed to our country. Today, nation states, criminal enterprises, and hacktivist groups alike can leverage sophisticated means to exploit unsophisticated vulnerabilities to conduct espionage, breach privacy, and wreak havoc on critical infrastructure, government systems, and businesses throughout the country. We are at a point where the stakes of defensive stagnation pose increasing risks in the face of threat actors' innovation. This is why it's so important to continually evolve in how we prevent, detect, and respond to cyber attacks.

Throughout my career, I have seen firsthand the challenges and opportunities of improving American cybersecurity from my work in the private sector, government, and academia. For nearly a decade, at CrowdStrike, a leading cybersecurity company, I have had a front row seat to cybersecurity innovation while building our privacy and public policy programs and advising customers around the globe. Prior to that I worked at the intersection of law and technology in the FBI's Office of the General Counsel. I previously taught at universities in the US and Europe, and currently serve as an adjunct professor in American University's cybersecurity policy program. I have been asked to speak here today from a stakeholder perspective. Accordingly, my testimony is informed not only from my experience but also by my continued engagement with government agencies through formal and informal advisory roles, including as a member of CISA's Joint Cyber Defense Collaborative (JCDC).

At CrowdStrike, we have a unique vantage point on cybersecurity threats and the innovation necessary to stop them. We not only protect 15 of the largest 20 banks in the US but also provide our cybersecurity technology and services to thousands of small and medium sized businesses. This means that it is not only possible for small organizations to leverage the same cybersecurity technologies as complex multinational enterprises but that it is becoming more common.

Increasingly, fundamental aspects of cybersecurity program design are applicable everywhere–including for the ongoing transformation in U.S. federal cybersecurity.

CrowdStrike works with CISA in a variety of ways across key programs and activities. We were one of the original plank holders of JCDC and remain active members to this day. We provide cyber threat intelligence and cybersecurity technology offerings to CISA that help it defend not only its own networks but those of some other government departments and agencies as well. Lastly, we are a consumer of CISA's advisories and a key technology provider for its other stakeholder groups, like critical infrastructure entities.

Key Developments

This hearing is timely for three key reasons. First, over the past couple of years CISA has reached its stride across a number of operational and planning functions (described in more detail below). Second, major transitions are taking place in federal cybersecurity overall, with an emphasis on security program modernization and Zero Trust Architecture. CISA is a key actor and implementer in these areas. Third, geopolitical conditions have yielded a worsening cyber threat environment overall. Russia's war in Ukraine and heightened competition with China are just two of several active examples where risks are mounting.[1]

Now is an impactful time to review the state of cybersecurity overall and evaluate CISA's considerable progress and contributions.[2] As DHS and CISA leadership and Members of this Committee prepare jointly to realize the vision of *CISA 2025,*[3] we can identify fruitful areas for continued development, alignment, and investment, where appropriate.

The State of Cybersecurity

Cybersecurity outcomes vary substantially across different sectors. Different sectors face different threats, have different constraints and capacities, and have different tolerances to risk or disruptions. To this end, I'd like to survey the state of cybersecurity across a few key CISA partner segments.

Federal Civilian Executive Branch (FCEB). Going back 20 years, Federal government agencies often had considerable cybersecurity strengths relative to their private sector counterparts. However, as time went on and cyber attacks increasingly occurred without the use of malware, parts of the private sector met and exceeded FCEB cybersecurity performance by adjusting to new realities. In some instances, government IT standards and controls failed to evolve at the rapid pace of innovation within the commercial IT and cybersecurity space. Large Federal Cybersecurity

[1] *See Adam Meyers, Testimony on Securing Critical Infrastructure Against Russian Cyber Threats,* House Homeland Security Committee (March 30, 2022) (How Russia-nexus adversaries use cyberattacks and recommendations for U.S. readiness), https://docs.house.gov/meetings/HM/HM00/20220405/114553/HHRG-117-HM00-Wstate-MeyersA-20220405.pdf.

[2] *See CISA Strategic Plan 2023-2025*, CISA (September 2022), https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf.

[3] *See CISA 2025 Overview,* Committee on Homeland Security, House of Representatives (October 13, 2022), https://homeland.house.gov/cisa-2025/.

programs (e.g., National Cybersecurity Protection System (NCPS) or EINSTEIN, and the Continuous Diagnostics and Mitigation Program (CDM)) set ambitious goals aimed to standardize and scale approaches to government cybersecurity, but even with considerable investment over the years, that aim remains unmet.

Over the past several years, however, the Federal cybersecurity community has made some significant strides. Recent developments are trending positively with the embrace of key cybersecurity concepts like centralized visibility of IT infrastructure to detect and respond to incidents. Significantly, E.O. 14028 on *Improving the Nation's Cybersecurity*[4] mandated the use across the FCEB of key best practices, like enhanced logging, as well as now-baseline technical solutions like Endpoint Detection and Response (EDR). The release of the Office of Management and Budget's *Federal Zero Trust Strategy*[5] in January 2022 was another key decision enforcing the use of sound approaches, like increased adoption of cloud-based technologies, credential management practices,[6] and defensible IT architectures. Even as implementation continues, these initial efforts are yielding positive results.

CISA plays an essential role in strengthening FCEB cybersecurity. As recently as a couple of years ago, CISA had just a few programs (e.g., NCPS, CDM, Trusted Internet Connections (TIC)) and a few authorities (e.g., Emergency Directives, Binding Operational Directives[7]) to meet this mandate. But the Solarium Commission's recommendation as enacted by Congress to formally elevate CISA to become the operational CISO of the FCEB, including by providing government-wide, proactive cyber threat hunting capabilities, considerably strengthened CISA's toolkit. Further, actions taken by CISA to implement E.O. 14028, particularly with regard to the EDR program, are helping to realize this vision.

The stakes are high. The FCEB continues to be a key target of threat actors that seek to do harm to the United States. Friends and allies continue to look to the U.S. Government as a model for how to organize their own government cybersecurity efforts. And importantly, the government must lead by example on cybersecurity. CISA's efforts to strengthen security across the other entities (e.g., critical infrastructure or state and local governments) will lack credibility if the FCEB is poorly secured.

Large Enterprises. On balance, the most sophisticated large enterprises in the U.S. have seen stronger cybersecurity outcomes in recent years, even as threats evolve and multiply. Over the past year, we've observed an increase in vulnerability reuse and increased reliance on access brokers to facilitate initial infiltration into target organizations. We've also witnessed increased targeting of–and mounting costs from–breaches of legacy infrastructure.[8] Supply chain attacks, which can be

[4] *See Executive Order on Improving the Nation's Cybersecurity,* The White House (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[5] *See M-22-09 Memorandum for the Heads of Executive Departments and Agencies,* Executive Office of the President, Office of Management and Budget (January 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[6] *See 7 TYPES OF IDENTITY-BASED ATTACKS,* CrowdStrike (January 10, 2023), https://www.crowdstrike.com/cybersecurity-101/identity-security/identity-based-attacks/.

[7] *See Cybersecurity Directives,* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/directives.

[8] *See 2023 Global Threat Report,* CrowdStrike (2023). https://www.crowdstrike.com/global-threat-report/.

targeted but also used to breach many dependent organizations in a single campaign, remain a key concern.

Some large commercial enterprises have greater flexibility and stronger security budgets than other entities, and thus serve as an important proving ground for new technologies, practices, and architectures. From this, recent innovations like Zero Trust and cloud-native EDR have become today's cybersecurity essentials. In the near future, we should expect more attention from other sectors on emerging enterprise security concepts like Extended Detection and Response (XDR), identity threat protection,[9] as well as continued adoption of managed security services (discussed in more detail below).

Small- and Medium-sized Businesses (SMB). These entities include everything from the family-owned corner store in each of our communities to startups creating new technologies that could change the world. These companies operate off of very different templates but nevertheless share two key features. First, resources are scarce. Second, a multi-day business disruption might well destroy the company. Resource scarcity means there's no place for complex cyber defenses, and few if any 'spare cycles' for participation in demanding or time-consuming information sharing initiatives. Sensitivity to disruption means these organizations are particularly vulnerable to ransomware and "lock-and-leak" attacks.

Among the most positive developments in this space in recent years is the growing affordability and accessibility of managed security services, as well as managed threat hunting services. Organizations increasingly look to professional providers to manage the overwhelming majority of defense actions–under tight service level agreements–24 hours a day, 7 days a week, 365 days a year.

State, Local, Tribal, and Territorial (SLTT) Entities. Over the past few years, SLTT entities have faced a withering threat environment, most notably from criminal ransomware actors. Materially all SLTT entities face budgetary and personnel constraints, and rely upon critical legacy applications and IT infrastructure. Nevertheless, over that same time horizon, cybersecurity outcomes within the sector have diverged significantly. As Members of this Committee know well, many SLTT organizations faced severe incidents and events, and in some instances citizens suffered disruption of key services.

Counterintuitively perhaps, over this timeframe the most forward-leaning states and cities were meaningfully further ahead than most of the FCEB in centralizing and modernizing defenses. This was generally achieved through a key service provider–typically a Department of Technology–implementing and managing transformative technologies like EDR and other important security concepts and practices. In addition to leveraging a centralized provider, these states often had no inflexible security program that acted as a barrier to experimentation and technology

[9] *See Andrew Harris, CrowdStrike Falcon Identity Threat Protection Added to GovCloud-1 to Help Meet Government Mandates for Identity Security and Zero Trust,* CrowdStrike (June 1, 2022), https://www.crowdstrike.com/blog/how-falcon-identity-threat-protection-helps-meet-identity-security-government-mandates/.

adoption. In addition, community-oriented support efforts, such as those led by the Center for Internet Security, have been a key part of stronger defenses.

The State and Local Cybersecurity Improvement Act, which passed into law in the Infrastructure Investment and Jobs Act of 2021 was a positive step in ensuring state and local governments have the funding needed to centralize and modernize cyber defenses. We appreciate former subcommittee Chairwoman Clarke, Chairman Garbarino, and other members of the committee for their leadership on this important issue.

Critical Infrastructure. Most critical infrastructure owners and operators face the same set of hardships outlined above: severe threat environment, personnel and budget constraints, and legacy applications and IT infrastructure. But they have the added challenges of complex Operational Technology (OT) that in some instances is obsolete and/or esoteric. In addition to these conditions there is increased interest from policymakers in regulatory measures designed to enhance cybersecurity.

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), signed into law in March 2022, which strengthens reporting obligations for critical infrastructure players, is the most meaningful step to date.[10] CIRCIA's authors–notably Members and key staff on this Committee–recognized these risks and included two key provisions. The first is a Cyber Incident Reporting Harmonization Council that should reconcile duplicative or conflicting regulations. The second is a generous timeline for CISA to articulate particulars (like thresholds) in a clear and straightforward manner. CISA has solicited stakeholder feedback to those ends, to which we, and many others in the community, were happy to contribute ideas and suggestions.[11]

International. Although somewhat beyond the scope of this hearing, we should take a moment to reflect on international cybersecurity. U.S. allies' public sector organizations, laws, and policy debates tend to reflect somewhat developments here in Washington. This is an incredible leadership opportunity. Efforts like the International Counter Ransomware Initiative[12] serve as a good example for how to use this influence to strengthen the cybersecurity ecosystem globally. Across relevant areas of law and policy, we should embrace interoperable approaches that simplify collaboration between governments, NGOs, and industry players. In addition, the U.S. should be receptive to areas where other countries have identified helpful policies. These include, for example, policies that support the startup ecosystem, and national privacy laws that simplify data protection and the cross-border data flows integral for modern cybersecurity.[13]

[10] *See Public Law 117 - 103, Division Y, Cyber Incident Reporting for Critical Infrastructure Act - Consolidated Appropriations Act, 117th Congress (March 15,* 2022). https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[11] *See CrowdStrike Response to RFI on Cyber Incident Reporting for Critical Infrastructure Act (November 14, 2022),* https://www.crowdstrike.com/wp-content/uploads/2023/02/RFI-Incident-Reporting-for-Critical-Infrastructure-Act-of-2022.pdf.

[12] *See International Counter Ransomware Initiative 2022 Joint Statement,* The White House (November 1, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/.

[13] *See Drew Bagley, Data Protection Day 2023: Misaligned Policy Priorities Complicate Data Protection Compliance,* CrowdStrike (January 27, 2023), https://www.crowdstrike.com/blog/data-protection-day-2023-misaligned-policy-priorities-complicate-data-protection-compliance.

Public-Private Collaboration

The Joint Cyber Defense Collaborative (JCDC). Information sharing in the cybersecurity space is a complex topic and longstanding policy priority. For two decades, various information sharing efforts–narrow and broad; informal, quasi-official, and official; *ad hoc* and enduring–have arisen from a desire within the cybersecurity community to do more. While the Cybersecurity Act of 2015 sought to address this problem head on,[14] structural impediments to comprehensive sharing and collaboration remain.[15] And as a practical matter, we are unlikely to identify a "silver bullet" solution to a problem with this many complexities. However, the formation of JCDC in August 2021 was a key development in promoting sharing and collaboration. In the time since, JCDC has created a platform for key players in industry and government to voluntarily work toward common goals.

While we would generally defer to CISA Leadership to describe key outcomes, we can say that CrowdStrike values the partnership opportunity. We continue to invest time and expertise in the JCDC community, and we look forward to continued, shared efforts to promote better cybersecurity.

As JCDC matures, we believe the effort can continue to improve. Two suggestions:

- **Consider approaches that stratify or segment membership to maintain trust**. As the group expands, JCDC leadership should account for the possibility that some members may become less willing to share details about sensitive issues. JCDC has addressed this concern by maintaining clear direct channels of communication with participants, and creating ad hoc working groups with a subset of members. These are important measures, but additional subgroup governance may help promote more active and applied sharing. Articulating long-term aims for membership composition may also be of value.
- **Strengthen *administrative* Customer Relationship Management (CRM) practices**. This would ensure consistent notification of participant stakeholders about upcoming opportunities, events, engagements, etc. A designated partner "JCDC relationship owner" should be able to flexibly add or remove corporate participants from various JCDC workstreams to facilitate participation from particular personas (e.g, according to function, experience, protocol, etc.).

To their credit, JCDC leadership and staff have been proactive about seeking feedback from participants. We have provided suggestions along these lines to them directly and believe it is taken seriously. Like any "startup," we anticipate continued iteration as the group matures into its full potential.

Ecosystem. CISA contributes to the cybersecurity ecosystem in a variety of other ways. Support to key partners in the SLTT community; advice and tools for enhancing infrastructure, Industrial

[14] *See Public Law 113-113, Division N, Cybersecurity Act of 2015.* 114th Congress (December 18, 2015), https://www.congress.gov/bill/114th-congress/house-bill/2029/text

[15] *See George Kurtz, Questions for the Record - Hearing on the Hack of U.S. Networks by a Foreign Adversary,* Senate Select Committee on Intelligence (February 23, 2021) (How the private sector has promoted practical information sharing),https://www.intelligence.senate.gov/sites/default/files/documents/qfr-gkurtz-022321.pdf.

Control Systems (ICS), and OT security; alerts and notifications for IT security, particularly around emerging vulnerabilities; and leadership on workforce topics all contribute to better cybersecurity outcomes. Each of these issue areas is complex and requires specific expertise. CISA's contributions in this realm continue to mature and become more valuable over time.

There remains a gap in cybersecurity performance between the "haves" and the "have-nots," which threat actors continue to exploit and which CISA cannot solve alone. To this end, we are pleased to see reference in the new National Cybersecurity Strategy to shifting the burden for cybersecurity to those best positioned to mitigate risks. This includes, where appropriate, holding platform providers accountable for the security of their products.[16] As a community, we should no longer tolerate certain software vendors externalizing the costs of–or worse, nakedly monetizing–insecure software applications.[17] While this policy concept must be made more concrete, a reasonable first step is ensuring that we're not rewarding vendors that cause harm. To this end, the government can lead by example by using its own procurement power to shape market dynamics. This is clearly a productive area for continued congressional oversight.

Recommendations

1. **The entire field must become more responsive in adapting to lessons learned**. Unfortunately, cyberattacks with the potential for systemic implications take place with increasing regularity. However, organizations are uneven in adopting key lessons, from new security controls and mitigations to more secure architectures. From our vantage point, key lessons of recent breaches include:

- Use managed security services where practical to augment internal security staff and attain responsive and comprehensive security coverage.
- Adopt cloud-based IT systems and where possible, leverage cloud-based security tools to achieve scalability and speed.
- Employ Zero Trust Architecture, with emphasis on identity threat protection, to defend an increasingly diffuse IT infrastructure and radically reduce lateral movement during breach attempts, bringing us closer to cyber and mission resiliency.

2. **We must approach regulation deliberately and harmonize to the greatest extent possible.** Even as CIRCIA advances through rulemaking, independent regulators are pursuing new obligations[18] and the National Cybersecurity Strategy foreshadows additional actions at the sector-level.[19] Each of these measures is well-intended, but taking place simultaneously and with different stakeholders. At best, they will close longstanding gaps and strengthen national resilience.

[16] *See National Cybersecurity Strategy, page 20.* The White House (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[17] For one example of a persistent security issue, see *George Kurtz, Testimony on Cybersecurity and Supply Chain Threats,* Senate Select Committee on Intelligence (February 23, 2021) (Extended discussion on emerging cybersecurity controls and practices), https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf. p. 5.

[18] *See TSA issues new cybersecurity requirements for airport and aircraft operators,* Transportation Security Administration (March 7, 2023), https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

[19] Even prior to CIRCIA and recent efforts, data breach victims commonly faced more than 50 different reporting requirements in the U.S. alone, with additional international obligations in many cases.

At worst, they risk yielding burdensome, distracting, and costly compliance obligations without additional security gains. Optimizing for the former is among the most important challenges the cybersecurity policy community faces at this time. Our hope is that continued collaboration between potential regulators and/or muscular harmonization efforts will help avert worse outcomes. The best advice we can offer is:

- Be deliberate about advancing new requirements;
- Provide formal commenting periods for stakeholders to contribute views;
- Use principles-based requirements rather than burdensome and inflexible compliance-based approaches;
- Include provisions to regularly review and if necessary modify, update, or deprecate requirements or controls based on developments in the threat environment or technology ecosystem;
- The DHS Cyber Incident Reporting Council established under CIRCIA should operate with vigor, and work to clearly identify and reduce duplicative reporting; and
- Set the goal of all federal agencies showcasing cybersecurity best practices with a particular emphasis on those that regulate cybersecurity "walking the walk."

3. **As a community, we should focus more attention on national incident response capacity.** JCDC should continue coordinating and developing community response plans and CISA should weigh potential JCDC contributions for the purposes of forthcoming revisions to the National Cyber Incident Response Plan (NCIRP).[20] If the Russian threat actors responsible for the major supply chain attack or the Chinese threat actors responsible for the Microsoft Exchange hacking campaign in 2021 had deployed ransomware or pseudo-ransomware at scale, large segments of the American economy would have been paralyzed. A CISA-administered program to retain outside providers for emergency incident response to attacks at entities of systemic importance could be of tremendous value in a future contingency.[21] This could mitigate crippling impacts and ensure CISA had the ability to orchestrate response activities and maintain insight into findings in real time.

4. **We must empower defenders with cutting edge cyber-defense capabilities.** Defenders with leading solutions are energized with radically improved morale. Too often, defenders are hobbled with inefficient and ineffective technologies. When these inevitably fail, they begin to feel like little more than a punching bag for adversaries, and that their best efforts are for naught. But when people are empowered, they can see their impact each day and can remain focused on the importance of their mission. To the extent that this Committee can promote access to better tools, that will absolutely strengthen cybersecurity outcomes. For the FCEB, this means the full adoption of technologies mandated in E.O. 14028 like EDR and, ultimately, better access to managed security services to augment staff. To highlight another opportunity, we believe it's time to have a more

[20] *See National Cybersecurity Strategy, page 12*. The White House (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[21] *See Robert Sheldon,Testimony on Protecting American Innovation, Senate Select Committee on Intelligence (September 21, 2022),* https://www.intelligence.senate.gov/sites/default/files/os-rsheldon-092122.pdf.

serious conversation as a community about using tax mechanisms to speed adoption of key technologies in the SMB space.[22]

5. **The community must attract and retain top cybersecurity talent.** The level of talent in our field–across industry and government–is deeply inspiring. Based on our experience, the central motivator for people in the field is a sense of mission. A key challenge we have as a community is overburdened staff leading to burnout, a concern that underpins some of my previous comments on leveraging managed services and mitigating time-consuming and ineffective compliance obligations. Further, aligning roles to each organization's key missions–and in the case of government authorities–helps people recognize the uniqueness of their contributions. A second challenge is expanding recruitment efforts to grow additional talent. To this end, I was pleased to announce during my participation at a White House Summit last month that CrowdStrike would soon launch an emerging leaders program focused on diverse candidates.[23] We must continue efforts to fuel the cybersecurity talent pipeline.

CISA's evolution is the culmination of non-partisan efforts under four consecutive presidential administrations, and CISA has received numerous new key authorities and increases in funding over the past several years. Ultimately, in each passing year it is important to ask whether the US government is better able to prevent, detect and respond to cyber attacks. Accordingly, I am pleased to see this committee has identified key oversight areas in the CISA 2025 initiative to put CISA on track to fully implement those authorities and fulfill the mission Congress has entrusted it with. CrowdStrike looks forward to continuing and building upon its trusted relationship with CISA, and playing our part in empowering it to effectively carry out its mission.

Thank you for the opportunity to appear in front of you today, and I look forward to your questions.

###

[22] *See Robert Sheldon, Testimony on Protecting American Innovation,* Senate Select Committee on Intelligence (September 21, 2022), https://www.intelligence.senate.gov/sites/default/files/os-rsheldon-092122.pdf.

[23] *See Readout: Office of National Cyber Director Hosts Roundtable on "The State of Cybersecurity in the Black Community"* The White House Briefing Room (February 28, 2023), https://www.whitehouse.gov/oncd/briefing-room/2023/02/28/readout-office-of-national-cyber-director-hosts-roundtable-onthe-state-of-cybersecurity-in-the-black-community/.