U.S. HOUSE COMMITTEE ON HOMELAND SECURITY
Subcommittee on Cybersecurity and Infrastructure Protection

Robert Sheldon
Sr. Director, Public Policy & Strategy
CrowdStrike

Testimony on "Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs"

September 19, 2023

Chairman Garbarino, Congressman Menendez, members of the Subcommittee, thank you for the opportunity to testify today. Materially all Federal government functions are predicated on operable information technology (IT) systems. Given that these functions include the provision of key services that underpin national security and our way of life, Federal cybersecurity is a topic of paramount importance.

CrowdStrike is a U.S. cybersecurity company, with employees across the country and globally. We bring a unique perspective on Federal cybersecurity issues. We are a provider of endpoint security technologies, cyber threat intelligence, and cybersecurity services to the Cybersecurity and Infrastructure Security Agency (CISA) and other Federal agencies. We are proud to be an original plank holder of CISA's Joint Cyber Defense Collaborative (JCDC). We also have unique perspectives from being a leading commercial provider serving major technology companies, 15 of the top 20 largest U.S. banks, and thousands of small and medium sized businesses.

Over the past two decades, the Federal IT enterprise has swelled in size and scope. No longer basic networks of desktops and servers, Federal IT today includes cloud workloads, mobile devices, Internet of Things (IoT) devices–and even specialized operational technology (OT).

In parallel, the volume and severity of cyber threats to Federal systems has increased. Nation state threat actors regularly seek–and too often, succeed—in breaching Federal enterprises. Over the past few years, major incidents have enabled adversaries like China and Russia to collect sensitive intelligence. In July, Chinese threat actors once again exploited authentication flaws in a major federal vendor's office productivity and email platform – this time resulting in threat actors' unauthorized access to the email of two Cabinet Secretaries.[1] Under slightly different geopolitical conditions or adversarial objectives, these incidents could have enabled scaled destructive attacks.

[1] See Nakashima, Ellen. Menn, Joseph. Harris, Shane. *Chinese hackers breach email of Commerce Secretary Raimondo and State Department officials.* The Washington Post, July 14, 2023. https://www.washingtonpost.com/national-security/2023/07/12/microsoft-hack-china/; and
Results of Major Technical Investigations for Storm-0558 Key Acquisition, Microsoft, September 6, 2023. https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

The evolution in the IT environment and worsening of the threat landscape mean it's important to regularly review and assess the efficacy of Federal cybersecurity measures–which include policies, programs, and strategies.

A Brief Background on CISA's Primary Federal Cybersecurity Programs[2]

By the early 2000s, Federal IT infrastructure had grown significantly. Cybersecurity protections were still fairly organic, with different agencies adopting different approaches, dedicating disparate resources, and achieving uneven outcomes. A significant uptick in cyberattacks targeting national laboratories, major defense industrial base entities, and the Federal government agencies themselves highlighted the need for greater investment and more standardization.

National Cybersecurity Protection System (NCPS[3]). Established in 2008, NCPS's goal was to protect Federal networks through a suite of perimeter defense technologies called "EINSTEIN," as well as an associated analytic capability. Leveraging intrusion detection and later intrusion prevention capabilities, EINSTEIN would attempt to defeat threats prior to threat actors accessing sensitive systems, like endpoints, or sensitive data. While the program clearly improved Federal cybersecurity posture from the status quo ante, and the associated analytic capabilities supported broader initiatives, EINSTEIN itself was not ultimately well-suited to meet the full scope of cyber threats to the ".gov."

Perimeter defenses are only one small part of cybersecurity. Two concepts help explain why. The first is the *assumption of breach*. Elite defenders have come to assume that threat actors can–and indeed, *already have*–breached perimeter defenses. Whether through a supply chain attack, malicious or unwitting insider, compromised identity, or any number of other methods, attacks often sidestep perimeter security measures and other defensive controls. Within this worldview, defenders must operate accordingly.[4] The second concept is *defense in depth*. This practice essentially layers defensive technologies to provide defenders multiple opportunities to detect and respond to threats. If a threat actor is able to breach the perimeter, defenses at the network, endpoint, and identity layers provide additional chances to stop them before they can achieve their objectives.

However useful EINSTEIN was at inception or at its peak efficacy, its value has eroded over time. Mobile devices, remote work, cloud applications, and other changes in the IT landscape have dissolved the perimeter, even as the increased use of encryption has complicated detection of malicious traffic at the perimeter-layer. Further, threat actors have become more adept in recent years at targeting endpoints, users, and identities directly. As a result, the security community–

---

[2] For brevity, I have not described broader Federal cybersecurity initiatives like Trusted Internet Connection program (2007), the Comprehensive National Cybersecurity Initiative (2009), FedRAMP (2011), the Federal Information Security Modernization Act (2014), or the Federal Information Technology Acquisition Reform Act (2014), but I would like to acknowledge their contributions to the Federal cybersecurity infrastructure that exists today.

[3] *See National Cybersecurity Protection System*, CISA. https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system.

[4] This assumption leads to the imperative to hunt, described below.

including government agencies and the White House[5]--have embraced concepts like Zero Trust, which essentially disavows the defensibility of the perimeter. While it's reasonable to maintain perimeter defenses as part of a layered security architecture for the ".gov," it's also reasonable to consider EINSTEIN a legacy technology and to focus investments elsewhere.

Continuing Diagnostics and Mitigation (CDM). By 2012, DHS had established a complementary, broader program called CDM. Rather than applying a uniform suite of protections across the ".gov," CDM would offer a flexible portfolio of technologies to defend Federal networks. The program would deliver new capabilities in four phases: Asset Management; Identity and Access Management; Network Security Management; and Data Protection Management.[6] A unifying requirement for tools acquired under the program is the ability to offer visibility through an integrated Agency-level dashboard, as well as an aggregated Federal-level dashboard.

Despite modest progress in early years, CISA officials report rapidly accelerating progress over the past few years. According to a recent CISA blog, "CDM is no longer a static effort to standardize agency capabilities and collect cybersecurity information, but rather the U.S. government's cornerstone for proactive, coordinated, and agile cyber defense of the Federal enterprise."[7] The post further credits Executive Order 14028 with strengthening the program's operational visibility, which highlights the addition of the Endpoint Detection and Response (EDR) program to CDM (explained in more detail, below). Further progress is possible with the extension of EDR to cloud workloads and mobile devices.

Recent Policy Developments

While the current major Federal cybersecurity *programs* administered by CISA are now 10-15 years old, Federal IT *policy* has accelerated. Stakeholders have made significant progress in the past few years, best illustrated by three key developments.

Threat Hunting Authorities. A central insight from the influential, bipartisan Cyberspace Solarium Commission Report of March 2020 was recommendation 1.4, which highlighted the need for CISA to perform *continuous threat hunting* across the ".gov."[8] P.L. 116-283, the FY21 National Defense Authorization Act (NDAA) Section 1705 granted CISA this authority, which positions the agency to act as the operational defender of the Federal government.[9]

---

[5] See Executive Order 14028, Improving the Nation's Cybersecurity, The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[6] *See CDM Program Overview*, CISA. https://www.cisa.gov/sites/default/files/publications/2020%252009%252003_CDM%2520Program%2520Overview_Fact%2520Sheet.pdf.

[7] *See Evolving CDM to Transform Government Cybersecurity Operations and Enable CISA's Approach to Interactive Cyber Defense,* CISA. July 23, 2023. https://www.cisa.gov/news-events/news/evolving-cdm-transform-government-cybersecurity-operations-and-enable-cisas-approach-interactive.

[8] *See Cyberspace Solarium Commission Report,* March 2020. https://www.solarium.gov/report, p. 41.

[9] *See NDAA Enacts 25 Recommendations from the Bipartisan Cyberspace Solarium Commission,* Sen. Angus King, January 2, 2021. https://www.king.senate.gov/newsroom/press-releases/ndaa-enacts-25-recommendations-from-the-bipartisan-cyberspace-

Executive Order (E.O. 14028). The May 2021 Executive Order on Improving the Nation's Cybersecurity advanced a suite of measures to further bolster security of the ".gov." Key among them were requirements to:

- Deploy Endpoint Detection and Response (EDR) capabilities, which among other things serve as the foundational enterprise cybersecurity technology for threat hunting;
- Implement Zero Trust Architectures, as well as generally accelerate cloud and Software-as-a-Service (SaaS) utilization;
- Standardize incident response practices; and
- Maintain more robust and consistent logging, which supports investigations and remediations.[10]

Federal Zero Trust Strategy. In January 2022, fulfilling a requirement from E.O. 14028, the White House Office of Management and Budget (OMB) issued a strategy for implementing Zero Trust across the ".gov." The memorandum identified specific outcomes and objectives that agencies must achieve over the coming years. This strategy serves a key roadmap that aligns industry and agency efforts over what will be a complex, multi-year process.[11]

Forthcoming Programmatic Developments

Budget request documents released over the past year foreshadow perhaps the most significant shift in the Federal cybersecurity program space since the advent of CDM. Specifically, CISA is in the midst of creating two new, closely-linked programs which will absorb elements of NCPS.[12] First, according to these documents, CISA will create a program called the Joint Collaborative Environment (JCE). At a high-level, JCE would split the NCPS program into two components. The first is EINSTEIN capabilities (i.e., perimeter defense), which would be maintained as legacy technology under JCE.

The second component of JCE is much broader–and is itself a meaningful new program–called Cyber Analytics and Data System (CADS). A summary document for the FY24 President's Budget Request describes CADS as "a system of systems[] that will provide a robust and scalable analytic environment capable of integrating mission visibility data sets and providing visualization tools and advanced analytic capabilities to CISA's cyber operators."[13] CADS would absorb the remaining

---

solarium-commission; and *The National Defense Authorization Act for FY 2021,* https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf, p. 695.

[10] *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/.

[11] *See Memorandum 22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,* Executive Office of the President, January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[12] This narrative draws on program descriptions within *CISA Budget Overview for FY 2024 Congressional Justification*. https://www.dhs.gov/sites/default/files/2023-03/CYBERSECURITY%20AND%20INFRASTRUCTURE%20SECURITY%20AGENCY.pdf. See also *CISA Strategic Plan FY 2024-2026*. https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf. For consistency, I have focused on characterizations from the President's Budget Request rather than from more recent but yet-to-be-finalized House and Senate Appropriations documents.

[13] *See Department of Homeland Security FY 2024 Budget in Brief.* https://www.dhs.gov/sites/default/files/2023-03/DHS%20FY%202024%20BUDGET%20IN%20BRIEF%20%28BIB%29_Remediated.pdf, p. 4.

analytic capabilities from the NCPS program, serve as the hub for Cyber Incident Reporting for the Critical Infrastructure Act of 2022 (CIRCIA) analytics, and support a number of other data-intensive operational activities.

Next Steps in Federal Cybersecurity

A core principle in cybersecurity is that the defender must have visibility into security-relevant events of the systems they defend. Today, this includes the endpoint, cloud, and identity planes in addition to the traditional network. Although stakeholders have made significant progress on Federal cybersecurity over the past few years in enhancing this visibility and control, several points stand out as next steps to further strengthen the security posture of the ".gov."

JCE and CADS implementation. Clearly, the JCE and CADS efforts described above will require a significant investment of time and resources. Federal cybersecurity programs historically have a long "shelf-life," and strengths and weaknesses can both compound over time. This underscores two key, future-oriented considerations:

- It's important to design these programs to enable flexibility. Changes in the IT or threat environment over time may precipitate the need to reallocate resources between program areas or initiatives.
- CADS in particular should be built for scale. The processing of data for cybersecurity purposes increased exponentially during the transition from the legacy antivirus age to the current EDR age. This trend could continue for some time, particularly as cloud workloads swell, log retention expectations increase, and adversaries and defenders alike seek to leverage Artificial Intelligence (AI). CISA must build CADS data processing capabilities that can perhaps double (or more) year over year for the foreseeable future.

CDM modernization and sustainment. With the realignment in NCPS described above, CDM will in a sense become the "mature" government cybersecurity program. This raises the question: at what point might CDM itself need to be modernized? From an operational standpoint, the EDR program has clearly breathed new life into CDM, so perhaps this is a question that can be resolved in the future. Nevertheless, when the time comes, stakeholders should consider two questions:

- While some EDR technologies were available through CDM prior to E.O. 14028, it ultimately required a mandate from the White House to deploy this essential technology across the ".gov." Cybersecurity professionals within CISA understood the importance of EDR, and it was clear that EDR would support CISA's hunting mandate. But CDM still works on the model of a catalog. In the future, is there scope for CISA to more proactively enforce the use of CDM technologies to fulfill its mission?
- Although, as noted above, EINSTEIN's operational capabilities have aged poorly, the NCPS program's architecture has aged like a fine wine. Specifically, it worked on a shared services model, meaning agencies got the benefit of EINSTEIN protections without complex budgeting or cost-sharing processes. With respect to the CDM program and associated funding, Federal CISOs still sometimes hesitate to acquire new technologies, given a real or perceived uncertainty about cost-sharing with CISA over time. In the future, is there scope

to adapt CDM, or elements thereof (e.g., EDR), to operate more directly as a shared service, where CISA funds the program for users directly?

Emerging cybersecurity capabilities. The cybersecurity industry is evolving at an uncharacteristically rapid rate. So over the next few years, the conversation within the Federal cybersecurity community will shift to new priorities. A few emerging areas to monitor, and further integrate into Federal defenses as appropriate, include:

- *Extended Detection and Response (XDR)*. Mature security programs within the private sector are already augmenting EDR to attain detection and response capabilities at other layers of the enterprise security stack. XDR enables visibility and control over network and identity (described below) data; the aggregation of logs; and the integration of threat intelligence within a unified workflow.
- *Identity Threat Detection and Response*. As security practitioners increasingly confront risks from IT ecosystem monoculture specifically, and identity-based attacks generally, there's greater interest in defending enterprises at the identity-layer. This emphasis comports nicely with broader Federal Zero Trust adoption efforts.
- *Artificial Intelligence (AI)*. While the application of AI to cybersecurity is not new, it is advancing. Although already resident within leading endpoint security tools, multiple other cybersecurity technologies will integrate AI and new AI-based capabilities will emerge over the coming years. This will drive speed, efficiency, and even make some tools more accessible through the integration of a natural language interface.[14] To the extent possible, Federal cybersecurity executives should view this opportunity holistically, consult broadly with industry and academia, and engage in long-term planning.
- *Managed Security Services*. Enterprises–even very large ones–increasingly leverage commercial managed security solutions. Defenders should be prepared to respond to and remediate cyber threats 24x7x365, and not all entities are able to build programs that can match the agility of dedicated commercial offerings. On the other hand, internal IT and security staff, by virtue of their trust and familiarity with the organization's mission space and constraints, are uniquely positioned to develop processes, address risks, and otherwise strengthen security maturity. So unburdening these internal operators from tactical demands on their time pays enormous dividends. This opportunity clearly applies in aspects of the Federal IT ecosystem.

Thank you again for the opportunity to testify today, and I look forward to your questions.

###

[14] See, for example, *Charlotte AI: Accelerate Cybersecurity with Generative AI Workflows* CrowdStrike. https://www.crowdstrike.com/products/charlotte-ai/.