**WRITTEN TESTIMONY OF STEPHEN ZAKOWICZ**

**VICE PRESIDENT**

**CGI FEDERAL INC.**

**BEFORE THE**

**SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION**

**U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY**

***"Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs"***

**SEPTEMBER 19, 2023**

## INTRODUCTION

Chairman Garbarino, Ranking Member Swalwell, and other distinguished members of the Subcommittee on Cybersecurity and Infrastructure Protection, my name is Stephen Zakowicz. I am a Vice President at CGI Federal Inc. ("CGI Federal"). As a wholly-owned U.S. operating subsidiary of CGI Inc. ("CGI"), [1] CGI Federal and its 7,100 employees partner with federal agencies to provide solutions for homeland security, defense, civilian, healthcare, justice, intelligence, and international affairs. During the last four years, I have served as the Project Manager on CGI Federal's contract with the Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") for the Continuous Diagnostics and Mitigation ("CDM") Program. On behalf of CGI Federal and its employees, I am pleased to submit this written testimony to the Subcommittee regarding the CDM Program.

CDM is a mission critical federal program that provides participating agencies with solutions and services to identify and combat cybersecurity risk. Since its original contract award in 2016, CGI Federal has provided this support to 100 participating agencies through tailored solutions and a robust shared services platform. CGI Federal is currently the prime contractor on two CDM Dynamic and Evolving Federal Enterprise Network Defense ("DEFEND") Task Orders - DEFEND C and DEFEND F. Under its DEFEND C Task Order, CGI Federal provides tailored CDM solutions to seven large Federal agencies: Department of Commerce ("DOC"), Department of Justice ("DOJ"), Department of Labor ("DOL"), Department of State ("DOS"), Federal Communications Commission ("FCC"), Tennessee Valley Authority ("TVA"), and United States Agency for International Development ("USAID"). Under its DEFEND F Task Order, CGI Federal developed a state-of-the-art cloud-based Shared Services CDM platform, and currently operates and provides access to that platform to 65 non-Chief Financial Officer Act ("CFO Act")

[1] 1 Founded in 1976, CGI is among the largest independent information technology ("IT") and business consulting services firms in the world. With 90,250 consultants and professionals across the globe, CGI delivers an end-to-end portfolio of capabilities from strategic IT and business consulting to systems integration, managed IT and business process services, and intellectual property solutions. CGI works with clients through a local relationship model complemented by a global delivery network that helps clients digitally transform their organizations and accelerate results.

federal agencies. Roughly 300 CGI Federal employees and subcontractors support the CDM program.

**CDM: Current Program Structure**

As stated in the DHS FY24 Congressional Budget Justification for CISA, "the CDM program provides the Department, along with other Federal agencies, with capabilities and tools to identify cybersecurity risks to agency networks on an ongoing basis. It prioritizes these risks based on potential impacts and enables cybersecurity personnel to mitigate the most significant problems first… Furthermore, CDM enables CISA and agencies to proactively respond to threats through the deployment of multiple different security capabilities, including data protection technologies, Endpoint Detection and Response (EDR), cloud security platforms, and network security controls, and enables CISA to continually evaluate the cybersecurity posture of [Federal Civilian and Executive Branch ("FCEB")] systems and networks."

As CISA describes on their public website, the CDM program is structured to provide cybersecurity protections and capabilities in four key areas:

- The Asset Management (AM) capability is aimed at providing agencies with a centralized overview of their network devices and the risks associated with such devices. Asset Management enables an agency to maintain and improve its cyber hygiene through five capabilities: hardware asset management (HWAM), software asset management (SWAM), configuration settings management (CSM), vulnerability management (VUL), and enterprise mobility management (EMM).
- The Identity and Access Management (IDAM) capability is intended to manage the access and privileges of agency network users. Managing who is on the network requires the management and control of account and access privileges, trust determination for people granted access, credentials and authentication, and security-related behavioral training.
- The Network Settings Management (NSM) capability is designed to provide agencies with greater visibility into what is happening on their networks, which also gives them a better understanding of how the networks are being protected.
- The Data Protection Management (DPM) capability is intended to provide additional protections to the most critical mission data and systems on federal civilian networks. While the other CDM capabilities provide broader protections across federal networks, the DPM capability is focused on protecting sensitive (especially private) data within the agency.

These capabilities are centrally managed and reported through the CDM Dashboard Ecosystem, a cloud-based visualization and data analytics layer that allows agencies and CISA to obtain a top-level view of cybersecurity risk posture and access details regarding how individual systems and endpoints contribute to that risk posture. This allows agency personnel to quickly identify and address the highest risk cybersecurity vulnerabilities first.

The current CDM program consists of seven individual Task Orders to provide consistent, prioritized CDM capabilities to FCEB agencies. Those Task Orders are:

- CDM DEFEND A: Providing CDM program requirements to DHS
- CDM DEFEND B: Providing CDM program requirements to DOE, DOI, DOT, OPM, USDA, and VA

- CDM DEFEND C: Providing CDM program requirements to DOC, DOJ, DOL, DOS, FCC, TVA, and USAID
- CDM DEFEND D: Providing CDM program requirements to GSA, HHS, NASA, SSA, and Treasury
- CDM DEFEND E: Providing CDM program requirements to DOED, EPA, FDIC, HUD, NRC, NSF, SBA, and SEC
- CDM DEFEND F: Providing CDM program requirements to up to 75 small and medium FCEB agencies through a Shared Services platform
- Dashboard Ecosystem: Developing and hosting a common CDM Dashboard platform on behalf of CISA to receive and consolidate information from participating CDM DEFEND agencies

**CDM Past and Present**

Since its inception in 2012, the CDM program has evolved to meet the priorities and relative maturity of the FCEB cybersecurity risk posture. When the CDM program began, it focused on implementing a standard set of commercial solutions to meet CDM-identified technical capabilities for enterprise visibility and protection. At that time, the program implemented cybersecurity risk management across the FCEB enterprise. Over time, however, the program recognized the need for flexibility to accommodate unique requirements and differing maturity levels from one agency to the next. Through CDM DEFEND, CISA addressed that need, and built a model focused on long term, sustained engagement, delivering custom solutions tailored to each agency's unique environments and cybersecurity needs.

Within the DEFEND model, CISA has further refined its approach to delivering cybersecurity services. For example, CDM DEFEND activities initially focused on delivering a single capability (e.g. Asset Management or Identity and Access Management) to all participating agencies. After deploying these foundational capabilities, CISA evolved to deliver services based on agency readiness model. In advance of agency engagement, CISA works with the agency to identify where program priorities align with an agency's ability to implement and maintain a specific capability. Using this readiness model, CISA validates that both CISA and the agencies are adequately funded and have the resources necessary to successfully deploy, operate, and maintain the cybersecurity solutions.

The evolution of the CDM program is also driven by new regulations and executive guidance. For example, Executive Order 14028 "Improving the Nation's Cybersecurity" (the "EO"), issued on May 12, 2021, provides greater visibility to agency environments as it grants CISA access to object level cybersecurity data collected through CDM (*see* Section 7(f)). The EO also authorizes CISA to engage in cyber hunt, detection, and response activities through Endpoint Detection and Response ("EDR") solutions deployed through CDM. These EO requirements grant CISA unprecedented visibility into agency network environments to proactively identify and remediate threats and apply observations in one agency environment across the FCEB enterprise.

Through the CDM program, CISA has gained critical visibility into the cybersecurity posture across the entire FCEB enterprise and is well-positioned to quickly identify, assess, and remediate potential threats to agency network environments and, by extension, U.S. national security. Specific accomplishments include the broad roll-out of EDR to FCEB agencies and the onboarding of roughly 250 CISA threat hunters to conduct analysis through EDR and CDM

Dashboard Ecosystem solutions. That access coupled with the availability of object level data through the Dashboard Ecosystem has been a "force multiplier" in providing CISA the ability to identify, assess, and remediate anomalies across the Federal enterprise network.

**Future of CDM**

CISA continues to evolve its CDM program to meet the needs of its stakeholders. Further, as CISA prepares for the next generation of CDM, it has actively engaged with industry and identified likely future priorities that include:

- Issuing Task Orders based on CDM capability to be applied across the entire FCEB community to promote consistency in solutions across agencies.
- Delivering CDM capabilities to State, Local, Tribal, Territorial (SLTT), and Critical Infrastructure (CI) stakeholders.
- Expanding access to Shared Services across CDM capabilities.
- Enhancing alignment and collaboration among CISA, FCEB agencies, and the cybersecurity tool vendor community.

**Concluding Observations**

As a federal contractor proudly supporting the CDM program, CGI Federal offers the following observations for consideration:

- Success of CDM's mission depends heavily on FCEB agencies applying the resources and funding to invest in cyber preparedness. Further, funding lapses or delays due to government shutdowns or Continuing Resolutions impact program continuity and ability to operate sustainably.
- Executive Order 14028 "Improving the Nation's Cybersecurity" enhanced CISA's ability to effectively perform its mission through, for example, authorizing CISA to engage in cyber hunt, detection, and response activities through EDR solutions deployed via CDM. Congress could ensure stability in CISA's authority to perform these critical activities by codifying these authorities into law.
- CISA could enable SLTT and CI stakeholders to leverage existing CDM shared service platforms and capabilities to defend against cyber threats such as ransomware attacks. These strategies would allow stakeholders to leverage valuable capabilities in a cost-efficient way to defend against threats such as ransomware attacks.
- The use of the Dashboard Ecosystem and EDR as a "first venue of consultation" for newly identified critical vulnerabilities or anomalous network activity by CISA represents a force multiplier and a new era of centralized hunt and response capabilities within the FCEB. These foundational capabilities can be further leveraged in innovative ways to improve our national security risk posture.

CGI Federal appreciates the critical nature of the CDM program, as well as CISA's core mission. CGI Federal is proud to support CISA and the CDM program in working to secure the federal government's networks for citizens across the United States. CGI Federal also thanks the Subcommittee for its continued oversight to ensure the continued success of the CDM program.

Written Testimony of:

Brian Gumbel

President

Armis, Inc.

Before the:

Committee on Homeland Security

Subcommittee on Cybersecurity and Infrastructure

U.S. House of Representatives

Regarding

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

September 19, 2023

548 Market Street, SUITE 97439
San Francisco, CA 94104-5401

1.866.695.1147
ARMIS.COM

Chairman Garbarino, Ranking Member Swalwell and Members of the committee, thank you for the opportunity to testify and share our perspective on civilian agency cybersecurity programs. I applaud the Committee's efforts in working to provide oversight and help improve impactful programs such as Continuous Diagnostics and Mitigation (CDM) and Einstein. In accordance with a core function of the NIST Cybersecurity Framework that highlights the need to go beyond merely identifying devices but also understand the interdependence each asset has with each other and their relative importance to business objectives, we are honored to bring a contextual asset intelligence platform to our customers, partners, and federal agencies.

Armis is THE leading asset intelligence cybersecurity company. We have been recognized by industry leading analysts and publications as a platform provider who brings a level of insight, awareness, and actionable intelligence to our customers. Today it is important to not only know what exists in your network and cloud infrastructure, but the interdependencies and vulnerabilities within each asset. We are honored to be under consideration to become a member of CISAs JCDC, sharing the mission and passion with all of you in ensuring the protection and security of our nation's critical assets.

We are encouraged by the focus and resources this committee and key agencies like CISA have put towards building dynamic, resilient and an effective cybersecurity framework in protecting these assets. On May 12, 2021, the Executive Order on Improving our Nation's Cybersecurity states "*Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life…" It mentions that "The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid." And that "The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety and national sovereignty (operational technology (OT)).*"

In the Armis State of Cyberwarfare and Trends report 2022/2023 where 6,021 IT security professionals where surveyed we found that 73% of IT professionals in the U.S. say their company has experienced one or more cybersecurity breaches. Threat activity against the global Armis customer base increased by 15% from September to November 2022 with the largest threat activity coming from critical infrastructure organizations followed by healthcare organizations as compared with other industries.

Our job as the industry leader is to raise awareness and identify areas in need of attention and improvement. Our experience has shown that intrusions outside traditional IT "managed devices" have become more prevalent. Programs and frameworks that in the past have been primarily focused on these managed devices will be limited in their ability to address the larger growing attack surface.

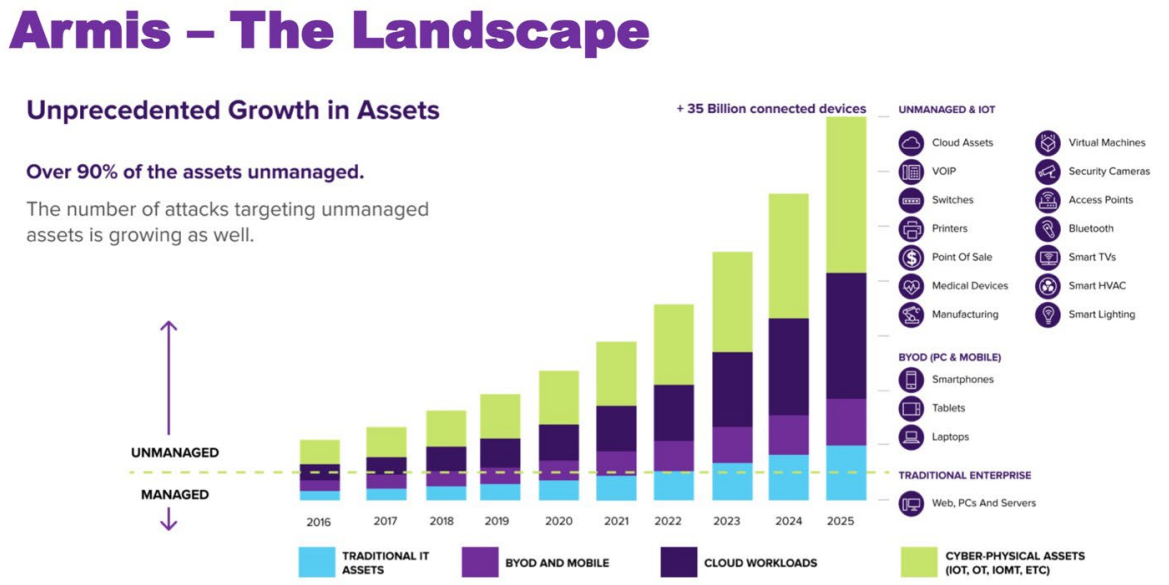
At Armis our comprehensive contextual intelligence engine includes over 3 billion assets and growing and includes the entire spectrum of IT/OT/IoT/IoMT assets. We bring a level of contextual asset intelligence to our customers that introduces a holistic and responsive platform to assist in their mission. Our public sector customers include several states, large city agencies and cities and counties as well as the following highlighted below:

- An agency within HHS as well as numerous State agencies leverages Armis for Asset visibility and intelligence through integrations.
- A large defense contractor leverages the Armis platform for Asset Discovery, Intelligence and Vulnerability Management
- A DOD agency leverages our platform for Asset Management and Security Workflow Remediation
- Department of Energy leverages Armis to increase automated identification and organization of the asset infrastructure across an entire lab.

Our enterprise and commercial customers include Drug and Manufacturing companies, Utility, Transportation, Aviation and Healthcare organizations, and many others.
Our mission is to help organizations understand where and what exists in their environments and help put them in a position to identify and manage vulnerabilities to respond rather than react to a breach. You can't protect what you can't see and without addressing a visibility gap, organizations cannot be fully prepared for the growth of today and uncertainties of tomorrow.

We work with organizations throughout the globe to gain complete visibility into their managed and unmanaged assets. A "whole of nation" approach cannot be achieved without a complete view and deep level of intelligence of both managed and unmanaged assets.

As you can see in the chart below, the growth and in our opinion the growing attack surface introduce vulnerabilities heretofore unseen and even unknown. The convergence of technologies and the dependencies between devices has introduced a more complex and challenging task for those who are responsible for securing critical assets and operational environments.




As stated in CISA's Binding Operational Directive (B.O.D.) 23-01, "Continuous and comprehensive asset visibility is a basic pre-condition for any organization to effectively manage cybersecurity risk." This directive focuses on Asset Discovery and Vulnerability enumeration. Many agencies and enterprises are fortunate to have strong endpoint technologies in place (EDR) and solutions that help protect the perimeter, but the attack surface continues to grow and the cybersecurity perimeter which was well defined just a few years ago is now dynamic and borderless. The introduction of unmanaged devices and operational technologies present challenges that cannot be addressed with legacy models and legacy technology. Present day challenges and national security threats are now implementing AI and automated capabilities to identify the weakest link in the chain. Automated threats from US adversaries requires automation and scalability delivering prioritization of cyber defense operators.

We applaud the activities towards the next generation Einstein program, Cyber Analytics and Data System (or CADS). According to CISA's Eric Goldstein *the system will integrate data from multiple sources, including "public and commercial data feeds; CISA's own sensors such as Endpoint Detection and Response, Protective [Domain Name System], and our Vulnerability Scanning service, which has thousands of enrolled organizations across the country; and data shared by both public and private partners,".*

Creating next generation programs are crucial and as our customers would attest, knowing where every asset exists, what the profile of that asset is, and whether it is aged, vulnerable, or compromised in real-time will help to make the investment in next generation and existing solutions more effective.

We are committed to continuing to work with CISA and other leading agencies to bring a holistic and inclusive approach where more complete and contextual asset awareness, contextual intelligence and attack surface definition can lead to increased resiliency and a responsive cybersecurity posture.

Some important and consistent feedback we hear from existing and former Federal CISOs, and CIOs includes the following:

"The focus should be on building modern security models, not perimeter based, and should acknowledge and focus on cloud, zero trust and IT/OT convergence.

"Many of the legacy models and contracts served us well in the past, but a new approach and model is needed."

These converged technologies deliver more efficiencies in the way we work but they introduce new vulnerabilities and complexities that legacy technologies are not built to identify, profile, or defend.

The "bold changes" highlighted in the EO call for a collaborative and inclusive programmatic and procurement directive that does not rely on legacy models, contracts, or solutions. What worked in years past will not suffice. Our adversaries are actively trying to exploit our visibility gaps, particularly in critical infrastructure. Our approach should be engaging with new and innovative 21st century technologies. Lest we forget, bad actors are moving at the speed of now as should we!

## Recommendations

- Design and implement a procurement path that allows for more expedient purchase and implementation of newer technologies built to align with the growing attack vectors and surface.

- Improve coordinating between programs like US Digital Services, the Technology Modernization Fund, and CISA to create programs which enable agencies to quickly integrate and maintain newer technologies and services into their framework portfolios.

- Fund the Technology Modernization Fund so that return on investments can reliably cover both the simultaneous deployment of new technology and the retirement of legacy services.

- Align program updates to stated directives. For example, if Directives state cloud-first and all assets, agencies should have the ability to implement those solutions that are not limited to a subset of technologies. Currently the CDM program addresses only IT devices rather than the full spectrum of connected risk: IT/OT/IoT/IoMT. BOD 23-01 focuses on Asset Discovery and Vulnerability Enumeration. Requiring that the full spectrum of converged and connected technologies be inventoried and reported would give these programs more alignment to stated Administration and Agency objectives. Having only **most** of your roof covered in a storm won't prevent water from entering!

- The CDM program and dashboard should reflect all existing and upcoming technologies that need integration vs. a limited few to be effective.

- We encourage continued strong support of the CDM program with the appropriate measures taken to be more inclusive of technologies that may not be part of the existing program.

Thank you again for the opportunity to speak with this committee. The resources of our entire organization stand ready to assist in the honorable mission of protecting our nation's most critical assets.

**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, headquartered in Austin, Texas 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/.

# United States House of Representatives

# Homeland Security Committee – Subcommittee on Cybersecurity and Infrastructure Protection

***Testimony of Mr. Joe Head – Co Founder and Chief Technology Officer, Intrusion, Inc.***

Good morning, and thank you Chairman Garbarino, Ranking Member Swalwell, and distinguished members of the subcommittee. My name is Joe Head. I am the cofounder and Chief Technology Officer of Intrusion – proudly headquartered in Plano Texas.

It is both a privilege and an honor for me to be here today, sharing my technical expertise and insights, which I have accumulated over four decades of immersion in the cutting-edge realms of the cybersecurity industry. I wholeheartedly commend the dedicated individuals on this subcommittee and their staff for their tireless efforts. They understand the need to enhance the Federal Government's cybersecurity capabilities but are also channeling their energies toward advancing the mission of agencies like CISA, with a strong focus on developing next-generation software and technologies that are critical in the forthcoming cyber conflicts.

I began designing and providing secure networks and other security solutions for the US Government when Ronald Reagan was President. We built equipment for the hot line from the White House to the Kremlin during his second term. I co-founded my company Intrusion in 1983, just 3 years out of college and we've been a public company since the 90's.

I've had more fun designing and securing things than you should get paid for. My goal today is to help the committee spur innovation in security. The US is not secure. There are some secure networks, but very, very few. Complacency with the state of our security is a serious risk. A relaxed defender is the most naïve one. Cyber offense is winning everywhere. A great challenge of our time is to make defenders better able to defend. I have an old friend who liked to say that he'd rather be lucky than smart. A network or system not breached is not a matter of the defender being lucky or smart, it is sadly that an attacker just isn't interested enough to focus on breaching it.

As you read my opening remarks, keep in mind that an outline of the Manhattan Project was not put in the Congressional Record before Los Alamos was built. Our government needs people with technical depth and a winning mindset. My job is not to inform our enemies what we plan to do to win the cyber war but to methodically ensure we take this domain. We do know what to do. There are core experts both in government and industry that understand what winning would require and how to get there. This path also includes how not to get there by spending billions unwisely.

Today I too often see security plans and programs looking a lot like children's soccer – a bunch of kids clustered around the ball. In cyber, the kids are always automating the hottest buzzwords without a grand plan to produce an absolute win. The challenge is to wisely architect a plan, put the right people in charge of defining the requirements, manage a design production, and reliably deploy a cyber get-well plan.

We must have a get-well plan in cyber which gets silently built and deployed, representing a master stroke in reversing the reality of our current predicament. Adversaries all over the world are killing it in cyber with massive asymmetry, winning and penetrating millions of systems that we need to be trustworthy. Many are capable hackers working inside adversary cyber operations or just as individuals on their own.

It was in the 1990's while identifying a threat at an automotive manufacturer that I realized we needed a better way to find the needle in the haystack. I built a database to understand what the Internet looks like, who owns what, which areas were unsafe to visit. This analytic engine has evolved into a mainstay of defense in depth cybersecurity. By the early 2000's we built a tool to inspect and audit Internet travels. Today, we know what traffic is coming and going from monitored systems, but more importantly how to stop threats from impacting operations.

Now is a critical time for the US Government, US critical infrastructure, and critical parts of US industry. If the world was awesome at cyber security, there wouldn't be a breach every 37 seconds. The more you know, the worse it looks. Is it hopeless, no. Is there reason to believe that the USG will naturally solve the problem, no. But the entirety of the nation faces continuous and advancing attacks precisely because of US commercial and governmental successes, so the USG must strategically cultivate protections.

As a student of history, we have seen dramatic examples of innovation in the face of new threats. There were dramatic examples in WW2 when foreign threats and war drove US innovation to new heights. Sadly, few programs in the cyber field are constructed to be game changers. Mostly they scale up and automate a few elements of a good security approach but are not master strokes of a comprehensive solution. In other words, when the projects are done you won't be truly secure. Well-automated partial solutions don't make you secure, they just delay risk and make companies poorer from the expenses. While we must improve our baseline defensive posture to exponentially increase the cost of attack, profit motivated hackers, criminals, and adversaries have already doubled-down on their attack investments with extensive resourcing.

We already know that signature-based defenses fall in the face of zero-days and basic offensive threats. Most defenses ignore attacks via trusted sources like supply chains and security tools. The adversary is operating faster than the decision cycle of defenders, hidden in the vast noise of network traffic. Similarly, most budget requests and coding projects are to scale up defenses that cannot see novel compromises that have never been seen before, much less stop these threats completely. We have the capability now to tell if the crown jewels leave on a path

headed for the shadows. With the advent of machine learning, network tools have identified and blocked untrustworthy sites, automatically guiding both people and devices to avoid the untamed internet, or offering them a picture of the monster rather than letting them directly reach out and touch it. But the unknowns must also be stopped, which requires knowing what good looks like.

Enemies are already exacting heavy costs on the US with cyber. Threats have been quietly planted into our infrastructure. Today – our country is still too reliant on foreign factories and vulnerable supply chains. The US does not make the computers, routers, switches, process controllers, dock cranes, pumps for gasoline, car parts, cameras, medicines, chemicals, and many other electronic things. But in cyber, it is much worse if your adversary made all the computers used in critical infrastructure or weapons systems. If your enemy left a back door or a designed-in a kill switch - they might use it. True security requires covering the supply chain threat as well as all other classes of threats like hackers and the insider threat.

Solutions

Why was I interested in testifying on this topic today? I believe that there is a chance that the US can re-achieve the needed sense of urgency these threats require. Investments in critical infrastructure, strengthening supply chains, and reshoring critical manufacturing are all necessary investments for our security. We must continue to be proactive in our approach to cybersecurity.

The allocation of over $400 million in funding for the transition from Einstein to CADS is a significant level of funding. It is imperative, however, that the CADS program design and implementation are meticulously executed to deliver not only enterprise-wide system monitoring and control but also the seamless handling of vast volumes of data and information. Intelligent and actionable outputs must be quickly and proficiently delivered to a broad audience. History has shown that well-intentioned technological advancements can be hindered by overly complex and convoluted designs, drowning users in a sea of tools and unnecessary complexity. We must keep in mind that offensive cyber operations can be cheap and flexible. Just like water can find any hole in a ship, building, or computer system and cause massive damage – a cyber attacker needs only to be creative enough to find or create one hole to get in and defeat you with cyber. We must remove those attacks from the shadows of the Internet, cut through that barrage of noise, and enable network defenders and analysts to discover the anomalies in the trusted high ground, where the maturing US cyber workforce can collaborate to investigate without having resources overwhelmed. We can start by identifying what good looks like. How should safe software and devices behave? Knowing these profiles drives proficient identification of threats.

Concurrently, we must remain vigilant against the pitfalls of comprehensive coverage leading to comprehensive failure. Adversaries will monitor our progress and respond. In the realms of design, application, and deployment, we must consistently ask ourselves how to intelligently

and efficiently innovate new capabilities and approaches into a far more effective solution. This ensures that our legacy solutions, designed to address legacy problems on a massive scale, are agile enough to perform effectively in real-world scenarios.

To achieve success, systems like CADS must work quickly, easily, and reliably. That is difficult. Solutions need to respond immediately to a threat, preventing outbound communications and impact to system operations. The response should be simple and as automated as possible – and not labor intensive – overwhelming our already-taxed defenders. Plans need to account for integration and sustainment at the outset. And be agile enough to know that new things will need to be included over time. Our systems need to be real-time, 24/7 without a nagging string of alerts. A system that is both powered by quality and comprehensive data.

Beyond the outside threats, the CADS system should support zero-trust principles to mitigate and uncover compromises of accounts and systems. Digitally this means understanding the following about a system and its users:

- Who are the users?
- How do they behave?
- What is their reputation?
- Who have they been associating with?
- What does normal activity look like for mission need?
- What are the indicators of malicious intent?
- What are common traits of targets for a particular attack?
- How can targets reduce their exposure before being targeted?

Moreover, it's essential to examine how a relatively modest investment in pioneering technologies and capabilities could potentially revolutionize our cybersecurity approach. By allocating funding to these "moonshot" endeavors, even in the order of a few million dollars, we may uncover the next major breakthrough in cyber defense, at a cost that pales in comparison to the budget required for comprehensive systems like CADS.

We strongly recommend these flagship programs and agencies acknowledge that without specific and targeted funding for strategic research and development, we run the risk of neglecting the cyber defenses necessary for the latter half of the 21st century. DOD does this with DARPA and other programs. That’s one model, but any substantial investment in major cyber defense programs, without accompanying funding for innovative and transformative technologies, could render these programs vulnerable. Much like the Maginot Line, an unforeseen breach in an inadequately defended area could undermine the entire defense system, rendering it futile and ineffective.

As I conclude my opening remarks, I would like to emphasize to the committee that while the introduction of the CADS system seems to represent a significant stride in the right direction, we must not let complacency take root. We should actively seek ways to complement the capabilities of CADS with innovative functions and useable systems that align with our overarching mission of fortifying the US cyber defense posture. By doing so, we can ensure that our nation remains at the forefront of cybersecurity, prepared to confront the evolving challenges of the digital age.

Just like the Manhattan Project would not have worked without a core team of geniuses backed up with a massive support and implementation program – now is as good a time as any to take charge. Congress can wisely pass laws and fund efforts that guide the course of this cyber conflict. We don't need to wait for our communications, power, logistics, and critical infrastructure to be taken offline in the lead up to a conflict.

Spending tens of billions on the latest partial buzzwords isn't a winning strategy, let's implement a winning cyber strategy on a tight timeline at an achievable budget. This path doesn't stop the kids' soccer teams from doing what kids do with massive pieces of federal budgets, so let's carve out 5% for a cyber Manhattan Project that surprises the world with a defensive cyber solution that came out of nowhere and reversed the asymmetry of this conflict which we are losing. Winning is better.

Thank you again Mr. Chairman and Mr. Ranking Member for inviting me into this subcommittee's discussion today. I would be happy to answer your questions.