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

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.

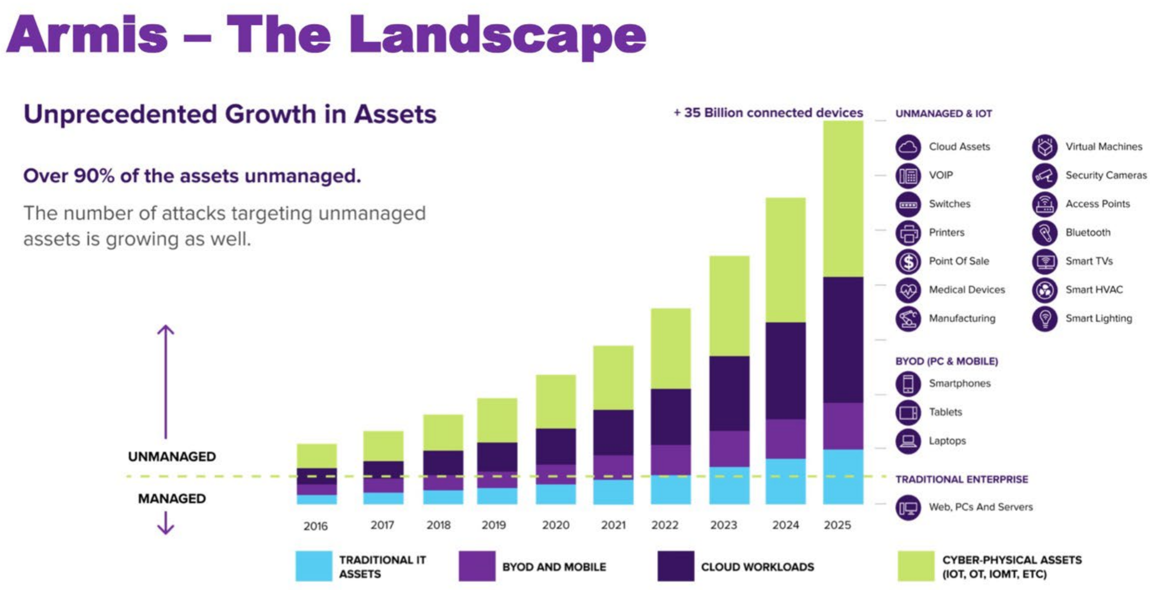
At Armis our comprehensive contextual intelligence engine includes over 3 billion assets and growing and includes the entire spectrum of IT/OT/IoT/IoMT assets. We bring a level of contextual asset intelligence to our customers that introduces a holistic and responsive platform to assist in their mission. 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.