Testimony

Jen Easterly

Director
Cybersecurity and Infrastructure Security Agency

U.S. Department of Homeland Security

FOR A HEARING ON

"National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems"

UNITED STATES SENATE

HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE

September 23, 2021

Washington, D.C.

Chairman Peters, Ranking Member Portman, and members of the Committee, thank you for the opportunity to testify on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) on our Nation's cybersecurity.

I am truly honored to appear before this Committee with our National Cyber Director and our Federal CISO. As I often say, cyber is a team sport, and Chris and Chris are certainly two of my best teammates. Let me begin by outlining CISA's priorities for accomplishing its mission, which include building and investing in our workforce, strengthening and defending federal networks, and working collaboratively with industry, both pre-event and in response and recovery. I will also share more information about our efforts to implement the President's Executive Order 14028, on *Improving the Nation's Cybersecurity*, and our perspective on cyber incident reporting legislation and FISMA reform. As I have shared with my team on just about each of my first 73 days, I have the best job in government.

First, people are CISA's number one asset. One of my principal goals is to make CISA the place where our nation's best cyber defenders want to work. I'm intently focused on building a culture of excellence that prizes teamwork and collaboration, innovation and inclusion, ownership and empowerment, transparency and trust. To that end, Secretary Mayorkas and I are committed to attracting and retaining world-class talent by implementing a vibrant, end-to-end talent management ecosystem that spans from recruiting and hiring, to onboarding and integration, mentorship and coaching, certification and training, recognition and promotion, to succession planning and retention.

Even as we focus on cultivating our workforce of today, it is important to recognize that our efforts also play an important role in helping build the cyber workforce of tomorrow. On November 15, 2021 the Department will launch the DHS Cybersecurity Service, also known as the Cyber Talent Management System (CTMS). Under the Secretary's leadership, the Department of Homeland Security (DHS) and CISA will use this system to grow the future cybersecurity workforce with greater flexibility to attract and retain the best cyber talent.

As one of the early women graduates of West Point, I have a deep appreciation for the importance of having diversity of background and experiences represented in the room when key decisions are made. That is why I am focused on keeping hiring centered around diversity by hosting specialized events, applying innovative sourcing techniques, and implementing branding campaigns as a means of attracting top talent. I will continue working to employ new and innovative recruitment and hiring strategies that cut the time to fill positions, reduce bias, and decrease unnecessary assessment while enhancing the diversity of our workforce. To that end, my goal is to make CISA a leader in diversity among both the Federal Government and the broader tech workforce.

Defending the Nation's Networks

In the wake of the recent Solar Winds and Pulse Secure campaigns targeting federal networks and the Colonial Pipeline and JBS Foods intrusions targeting our nation's critical infrastructure, we are working to address our nation's shared cybersecurity risk. We must collectively and with great urgency strengthen our nation's cyber defenses, invest in new

capabilities, and reimagine how we think about cybersecurity to recognize that all organizations are at risk and our efforts must focus on ensuring the resilience of essential services. To that end, as the National Coordinator for critical infrastructure security and resilience, CISA is acting with utmost resolve to drive reduction of cyber risk across Federal networks and the National Critical Functions. Achieving the outcomes we seek will require progress in several key areas.

First, CISA is currently investing in, and growing capabilities to increase visibility into cybersecurity risks across federal agencies and our critical infrastructure partners. As we all know, if we can't see it, we can't defend it. Therefore, we must enhance our ability to detect potentially nefarious network activity before it becomes systemic. This approach embodies a fundamental change, in which CISA conducts persistent hunts for threat activity, ingests and analyzes security data at all levels of the network, and conducts rapid analysis to identify and act upon identified threats. CISA leverages the results from threat hunting for adversary activity to inform its efforts to protect both federal networks and critical infrastructure, as the results from reported insights helps to drive our efforts, regardless of sector. At the same time, CISA is driving adoption of defensible network architectures, including implementation of zero-trust environments in which the perimeter is presumed compromised and security must focus on protecting the most critical accounts and data. Going forward, we must take lessons learned from our investments in federal cybersecurity to support organizations across sectors in driving similar change.

Second, CISA is working with all partners to gain increased visibility into national risks. With increased visibility, we will be able to better identify adversary activity across sectors. By identifying cross-sector trends, we can produce more targeted guidance and identify earlier how to prioritize and scale any potential response. As one element of this effort, CISA offers a pilot program called CyberSentry, which deploys technologies and analytic capabilities to monitor activity between business (IT) and operational technology/industrial control system (OT/ICS) networks for sophisticated threats. CyberSentry is a voluntary partnership with private sector critical infrastructure companies. This capability is not a replacement for commercial solutions; rather, the capability complements such solutions by allowing CISA to leverage sensitive threat information already being captured by network defenders. CyberSentry has shown significant benefit in practice and has been used to drive urgent remediation of threats and vulnerabilities.

Third, CISA continues to invest in and mature our voluntary partnerships with critical infrastructure entities. These partnerships with industry enable us to better understand the nature of vulnerabilities pre- and post-disclosure and in turn provide timely and thorough mitigation guidance to government agencies and critical infrastructure. CISA collaborates with private industry on significant risks, developing sector and threat focused products, and providing briefings on new trends, threats, and capabilities across the sectors.

The newly established Joint Cyber Defense Collaborative (JCDC) is building on these partnerships to lead the development of the Nation's cyber defense plans by working across the public and private sectors to help defend against cyber threats to the nation. Authorized in the National Defense Authorization Act for FY 2021, the JCDC brings together the authorities, capabilities, and talents of the interagency – CISA, the National Security Agency, the Federal Bureau of Investigation, Cyber Command, the Department of Justice, and the Office of the

Director of National Intelligence – with the power of industry to enable shared situational awareness of the threat landscape, to plan and exercise against the most significant threats to the nation, and to implement cyber defense operations against these threats. This new collaborative promotes national resilience by coordinating across federal agencies, to include Sector Risk Management Agencies (SRMAs); state, local, tribal and territorial (SLTT) partners; and industry to protect against, identify, detect, and plan for and respond to malicious cyber activity targeting U.S. critical infrastructure. Finally, the JCDC will leverage CISA's broad authorities to share information about threats and vulnerabilities to enable early warning and prevent other victims from being attacked. This shifting paradigm will enable us to transform information sharing into information enabling – timely, relevant, and actionable.

Cyber Executive Order Implementation Update

As you are aware, on May 12, 2021, President Biden signed Executive Order 14028, *Improving the Nation's Cybersecurity*. This Executive Order aims to directly address the persistent and increasingly sophisticated malicious cyber threats the nation has faced over the past several months, and tasks federal agencies to make bold, large-scale changes to improve the nation's cyber posture. The efforts outlined in the order aim to improve Federal cybersecurity posture and incident response capabilities, limit supply chain risk to the Federal government, and increase CISA's visibility across Federal and contractor networks. CISA has been tasked with leading, consulting, or supporting over 35 unique efforts, many with short timelines highlighting the criticality and urgency of the work to be done. I am proud to say that CISA met all of our deadlines in support of the Executive Order, to include:

- Driving adoption of modern, secure, and resilient networks, including through the Cloud Technical Reference Architecture, released for public comment earlier this month and co-developed with the U.S. Digital Service and GSA's FedRAMP program;
- Raising the bar for incident response by publishing a Vulnerability and Incident Response Playbook, which will ensure that all agencies will operate from the same sheet of music during incidents, and allow CISA to confidently coordinate a whole-of-government incident response effort, building on lessons learned in recent incidents;
- Ensuring that CISA has access to all necessary information about incidents affecting federal agencies by providing recommendations to the Federal Acquisition Regulatory Council that require broader sharing of data in response to incidents with the contracted agency as well as with CISA, and establishing procedures for sharing appropriate information with interagency partners to aid in their collective ongoing cyber defense operations;
- Establishing a plan to dramatically expand our visibility into cybersecurity risks affecting federal networks through deployment of endpoint detection and response (EDR) capabilities and enabling "persistent hunt" activities as authorized by Section 1705 of the FY21 National Defense Authorization Act; and
- Prioritizing federal supply chain security by directing a review of over 650 unique cybersecurity related contract clauses in place across the agencies and recommending

to the FAR Council a baseline for cybersecurity that Federal contractors must meet to lower risk to the Federal systems they support.

The work outlined in the Executive Order is no small task; the Administration asked CISA and agencies to rethink how we approach vulnerability and incident response, how we approach purchasing IT goods and services, how we design and secure our networks, and how we work together to share information. Our work applies not only to the federal government, but also to government at all levels, and the private sector, as we seek to work to ensure that we collectively drive adoption of strong security practices to materially reduce cybersecurity risks.

Cyber Incident Reporting Legislation

Facing repeated attacks on our Nation's Federal networks and critical infrastructure, CISA will continue to pursue ways to increase visibility into federal and critical infrastructure networks. We must also continue to rely on network owners and operators to identify and report anomalous and potentially nefarious activity on their networks to CISA and our partners.

Although some reporting requirements exist within certain sectors, there is currently no single mandatory federal requirement to report cyber incidents. Rather, entitities must assess the complex disclosure requirements imposed by an array of agencies at the Federal and State levels. Moreover, when a victim does seek to do the right thing and report an incident to the Federal government, they may not know which agencies to contact, delaying their reporting during an emergency situation. Among the harms this may cause is a lag in availability of critical mitigation guidance to the operators who are positioned to take action.

We appreciate the work of members of Congress in both the House and the Senate who have drafted or introduced bills on cyber incident notification over the past several months, including members of this Committee. The earlier that CISA, the Federal lead for asset response, receives information about a cyber incident, the faster we can conduct urgent analysis and share information to protect other potential victims.

To that end, cyber incident reporting must be timely, ideally within 24 hours of detection. Reporting should be broad-based, and not limited by type or sector, with CISA and DOJ having the joint authority, in coordination with other relevant departments and agencies, to set reporting thresholds and requirements for covered entities. These entities include critical infrastructure, federal agencies, and government contractors. It should also provide clear and compelling enforcement mechanisms that ensure compliance. We encourage Congress to adopt a cyber incident notification reporting approach that appropriately focuses broadly on cybersecurity incidents, including cyber supply chain and ransomware attacks, and provides CISA and DOJ, in coordination with other relevant agencies, the flexibility to modify the scope of the requirements as necessary, balancing the benefits of reporting against burdens to industry and government.

Federal Information Security Modernization Act (FISMA) Reform

Lastly, I'd like to thank the Chairman and the Ranking Member for your efforts to review and update the Federal Information Security Modernization Act or FISMA. Enacted in 2002,

FISMA, it recognized the importance of information security, and defined roles and responsibilities for the Federal Government. However, the rapid evolution of both technology and vulnerabilities are outstripping a policy-to-implementation process last updated in 2014. When faced with threats and vulnerabilities, corrective action can be stifled, especially when incidents span multiple agencies. Disparities in senior leadership engagement and cyber expertise across federal agencies, resource constraints, and a complex policy and governance environment impair risk management efforts. These hurdles are even more challenging since the networks supporting federal agencies are difficult to defend due to design, age, and insufficient investment.

In this operating environment, the legal framework governing management of Federal information security must enable all of government to lean into these challenges to seek effective, efficient, and coordinated solutions. However, in its current form, FISMA reflects the roles and responsibilities of nearly a decade ago, while the Federal Government still struggles to affect the level of oversight, accountability, and performance that was envisioned in FISMA 2014. There have been many changes in the intervening years, including the establishment of CISA, and the creation of the National Cybersecurity Director as part of the 2021 National Defense Authorization Act. Together with my teammates in cybersecurity, Chris Inglis, the National Cyber Director and Chris DeRusha, the Federal CISO, we stand ready to tackle the challenges facing the federal cybersecurity enterprise together. Clearly, the status quo is not acceptable. I welcome efforts by Congress to modernize FISMA to address the dynamic and challenging cyber landscape, targeting strengthened risk management and implementation, and recognizing CISA's role as the operational lead for federal cybersecurity.

CISA is appropriately positioned to identify and address unacceptable risk within and across Federal civilian executive branch agencies. CISA has the capability, expertise, and access to define and drive the right level of security to protect federal agencies in coordination with the Office of Management and Budget, the National Institute of Standards and Technology, and the National Cyber Director. Existing and planned CISA shared services, as well as continued modernization of our flagship cyber programs, namely the Continuous Diagnostics and Mitigation Program and National Cybersecurity Protection System, will provide an avenue for agencies to confidently enhance their own cybersecurity capabilities, where they are working, and also provide a backstop for agencies struggling to fill capability gaps. CISA is modernizing National Cybersecurity Protection System capabilities to support the increasing adoption of cloud services and other emerging technologies and improve CISA's ability to collect, process, analyze, and share cyber data with its partners. CISA will have a single analytical environment scaled to support the full spectrum of our services.

A modernized FISMA should shift the spotlight from compliance to risk management and implementation. This approach has led to an operating environment with heavy compliance requirements that do not always contribute to the intended outcome and in some cases distract from it. Instead, an environment that fosters implementation should ensure that cybersecurity actions enable agency missions and that agency leadership decisions appropriately prioritize and fund the security of their systems and networks.

We at CISA look forward to working with Congress to modernize FISMA to better align with the realities of modern information security, enabling a more effective Federal government through an updated law that balances security and reporting, and empowers information security leaders. As this effort moves forward, I will remain committed to working with my fellow agencies to champion the defense and security of federal systems.

Conclusion

Our nation faces unprecedented risk from cyber attacks undertaken by both nation-state adversaries and criminals. Now is the time to act – and CISA is at the center of our national call to action. In collaboration with our partners and with the support of Congress, we will make progress in addressing this risk and maintain the availability of services critical to the American people.

Thank you again for the opportunity to appear before the committee. I look forward to answering your questions.