
**Testimony**

**Jen Easterly**

**Director**
**Cybersecurity and Infrastructure Security Agency**

**U.S. Department of Homeland Security**

**FOR A HEARING ON**

# Evolving the U.S. Approach to Cybersecurity: Raising the Bar Today to Meet the Threats of Tomorrow

**UNITED STATES HOUSE OF REPRESENTATIVES**

**HOMELAND SECURITY COMMITTEE**

**November 3, 2021**

**Washington, D.C.**

Chairman Thompson, Ranking Member Katko, and Members of the Committee, thank you for the opportunity to testify on how the Cybersecurity and Infrastructure Security Agency (CISA) is positioned to enhance the security and resilience of our Nation's federal networks and critical infrastructure.

I am truly honored to appear before this Committee today to share my vision for CISA. Since being sworn in as Director in July, I continue to be impressed with the talent, creativity and enthusiasm of the dedicated CISA employees I am entrusted to lead. As I have shared with my team every day, I have the best job in government.

At CISA, our mission is to lead the National effort to understand, manage, and reduce cyber and physical risk to our critical infrastructure. Our vision is a secure and resilient critical infrastructure for the American people. At the heart of this mission is partnership and collaboration. Securing our Nation's cyber and critical infrastructure is a shared responsibility, and has never been more important than it is today. At CISA, we are challenging traditional ways of doing business and are actively working with our government, industry, academic, and international partners to move from traditional public-private partnerships to public-private operational collaboration.

**Who We Are**

Established by the CISA Act of 2018, CISA is the Nation's Cybersecurity and Infrastructure Security Agency.

While our programmatic mission areas deal in cyber defense, infrastructure security, and secure and interoperable communications, holistically, as one CISA, the organization is comprised of teams of individuals with expertise across a wide spectrum of professional backgrounds and disciplines. Each and every one of them rely on each other to achieve our shared objectives. We recognize the connective tissue that binds us together and ensures we are able to be successful in our mission to lead the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day. Our core values represent the fundamental tenets of our CISA organization: collaboration, innovation, service, and accountability. Living these core values every day with a growth mindset are the pathways to our mission success.

To achieve success in our cybersecurity mission, we build the national capacity to defend against cyber attacks and work with our federal partners and provide them with cybersecurity tools, incident response services, and assessment capabilities to safeguard the federal civilian executive branch networks that support our Nation's essential operations. We strengthen our Nation's cyber defense by leading asset response for significant cyber incidents and ensuring that timely and actionable information about known cyber threats and incidents is shared with federal and state, local, territorial, and tribal (SLTT) officials, as well as our international and private sector partners, to ensure the security and resilience of our critical infrastructure.

Within our infrastructure security mission, we enhance the protection of critical infrastructure from physical threats through enabling risk-informed decision-making by owners

and operators of critical infrastructure. Our activities include conducting vulnerability assessments, facilitating exercises, and providing training and technical assistance nationwide. Our infrastructure security program leads and coordinates national efforts on critical infrastructure security. This includes reducing the risk of successful attacks against soft targets and crowded places, such as in our schools, and from emerging threats. CISA also leads efforts to secure our Nation's chemical sector infrastructure, enhancing security and resilience across the chemical industry to reduce the risk of hazardous chemicals being weaponized. To this end, CISA has developed voluntary and regulatory programs and resources to help stakeholders—private industry, public sector, and law enforcement—secure chemical facilities from many threats: malicious cyber activity, biohazards, insider threats, and theft and diversion.

Key to success in our cybersecurity and infrastructure security mission is identifying and understanding risk, especially risk that is systemic to our Nation's critical networks and infrastructure. CISA's National Risk Management Center leverages sector and stakeholder expertise to identify the most significant risks to the nation, and to coordinate risk reduction activities to ensure critical infrastructure is secure and resilient both now and into the future. The goal of the NRMC is to create an environment where government and industry can collaborate and share expertise to enhance critical infrastructure resilience by focusing on collective risk to National Critical Functions including through key initiatives such as election security, Fifth Generation Network technology, supply chain risk mitigation, and more.

Our emergency communications mission works to ensure reliable and resilient, real-time information sharing among first responders during all threats and hazards. CISA enhances national security and public safety interoperable communications at all levels of government across the country through training, coordination, tools, and guidance. We lead the development and implementation of the National Emergency Communications Plan to maximize the use of all communications capabilities available to emergency responders—voice, video, and data—and ensure the security of data and information exchange. CISA assists emergency responders and relevant government officials with communicating over commercial networks, using priority telecommunications services during natural disasters, acts of terrorism, and other man-made disasters.

Underpinning our mission is CISA's commitment to preserving individual privacy, civil rights, and civil liberties protections in our operations and our engagements. We recognize that when Congress statutorily required CISA to have a privacy officer for the agency that we needed to—by default—fully integrate privacy, civil rights, and civil liberties protections into everything we do. We are proud of the fact that a number of our activities have the added benefit of enhancing privacy, civil rights, and civil liberties.

**Threat Landscape**

In our globally interconnected world, our critical infrastructure and American way of life face a wide array of serious risks with significant real-world consequences. Today, the critical functions within our society are built as "systems of systems," complex designs with numerous interdependencies and systemic risks that can have cascading effects. This is something we have known for years as nation-state actors and criminals increasingly leverage both cyberspace and

traditional physical means in their attempts to subvert American power, American security, and the American way of life. Many of these challenges are exacerbated by the COVID-19 pandemic, which has led to an unprecedented number of Americans working from home, meaning the potential for malicious actors to exploit vulnerabilities has expanded exponentially. Additionally, we are realizing the impact of climate change on our national security and economic prosperity interests, and must work with the infrastructure security and resilience community to mitigate them—through planning efforts that include community resilience, and a whole of government guidance and information sharing effort.

At the same time, ransomware has become a scourge on nearly every facet of our lives, and it's a prime example of the vulnerabilities that are emerging as our digital and our physical infrastructure increasingly converge. Earlier this year, we saw the Colonial Pipeline attack shutter gas stations along the East Coast and the JBS attack cause certain food prices to rise. We have also seen ransomware attacks on schools, police departments, hospitals, and small businesses around the country, and they are growing in number, scale, and sophistication. Disrupting this scourge requires a whole-of-nation effort, and the Department of Homeland Security (DHS) helps lead that effort, and led the development of a whole-of-government website, stopransomware.gov, which provides users with a central, authoritative source for guidance, toolkits, and other resources from across the Federal Government. CISA's mission focuses on raising awareness before disaster strikes, and supporting victims when it does. We help potential victims understand their risk, reduce vulnerabilities, and mitigate the impact if they are attacked. When attacks threaten our critical infrastructure or national critical functions, we offer on-site assistance to help victims get back on their feet and share operationally-relevant information with our partners and the public to prevent the spread to other potential victims and sectors. Our partners can use these resources to reduce the risk and impact of ransomware attacks.

While cyber intrusions and ransomware dominate the recent headlines, physical threats to our people and our critical infrastructure remain a top concern. Terrorism, mass shootings, and other forms of targeted violence continue to threaten our schools, places of business, houses of worship, and other soft targets and crowded places. In 2020 alone, there were more than 12,000 explosive-related incidents and more than a 70% increase in domestic bombings, according to the Department of Justice's U.S. Bomb Data Center. These types of physical threats can cause mass casualties, lead to hundreds of millions of dollars in damage, and cause cascading damage across vital physical and cyber infrastructure. From a broader perspective, as modern threats become more sophisticated, it is important to stay vigilant and take proactive measures to enhance the security and resilience of our communities and critical infrastructure.

The risks we face today are complex. They are dispersed both geographically and across a variety of stakeholders. They are challenging to understand, and even more difficult to address. But here at CISA we have an incredible team ready to execute our mission in collaboration with a diverse group of partners across all sectors. CISA will continue to support and empower our partners to secure and defend America's cyber ecosystem and critical infrastructure. While we face an array of cyber and physical threats, our adversaries continue to push mis- and dis-information in an attempt to divide Americans and cast doubts about the legitimacy of our elections and our democratic processes, among other issues. These are just a few of the threats

we face, and tackling them is no easy feat. It will take teamwork and a relentless dedication to our mission. Fortunately, in my first 100+ days at CISA, it's become clear that we are up to the challenge.

**Priorities**

For me, it was clear from my first days as Director that people are CISA's number one asset. My goal is for CISA to be the place where our Nation's best cyber defenders and security professionals want to work. I am 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, we are committed to attracting and retaining world-class talent by implementing a vibrant, and providing an 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, and 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 Cybersecurity Talent Management System (CTMS) and begin hiring employees in the DHS Cybersecurity Service (DHS-CS). DHS, including 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. My vision is to make CISA a leader in diversity among both the Federal Government and the broader tech workforce.

Collaboration to achieve these workforce and diversity goals is fundamental. So are our efforts to build relationships, trust and connectivity with state and local officials, private sector, and our interagency partners. CISA is meant to be an agency that is agile, flexible and able to respond quickly to changing threats through collaboration with both the public and private sectors. And, to this end, we sustain our trusted and effective partnerships between government and the private sector, which are the foundation of our collective effort to protect the Nation's critical infrastructure. With large portions of critical infrastructure in our country owned and operated by the private sector and municipalities, those partnerships are vital to ensuring a safe and secure America. Our partners bring expertise and a unique ability to drive climate change impact and cyber defense activities in their jurisdictions, and it is precisely this assembly of knowledge that will allow us to be better prepared to achieve deep operational collaboration that ultimately reduces the greatest risks to our Nation.

**Updates and Accomplishments**

There is a lot of good work being done at CISA. I am particularly proud of the Agency's efforts to stand up a new initiative called the Joint Cyber Defense Collaborative or JCDC, meet important deadlines from President Biden's Executive Order on Improving the Nation's Cybersecurity, and expand and strengthen key partnerships during my first 100 days. Allow me to elaborate on each of these accomplishments.

In August, CISA launched the JCDC, which unifies cyber defense capabilities currently spread out across multiple federal agencies, many state and local governments, and countless private sector entities. It also leads the development of our Nation's cyber defense plans by working across the public and private sectors to unify deliberate crisis and action planning, while coordinating an integrated execution of these plans. Our goal with the JCDC is to bring together key federal partners with private sector and SLTT partners who have critical visibility and ability to understand the threat landscape by virtue of their businesses and responsibilities, and to plan and exercise against the most serious threats to our nation.

The JCDC's initial focus is on tackling ransomware and developing a planning framework to coordinate incidents affecting cloud service providers. Almost two months into this collaboration, we are already seeing good progress. Our relationships with our private sector partners continue to grow as we share more information and collaborate around key operational issues. We are also validating and sharing information daily across broad swaths of partners in multiple sectors. For example, last month, CISA, the Federal Bureau of Investigation, and the National Security Agency issued guidance to help critical infrastructure entities protect themselves against BlackMatter ransomware as a service, using information provided by JCDC members.

While it is early days, the JCDC is already leveraging the skillsets, expertise, capabilities and visibility of its members to better protect critical assets against cyber threats. This shifting paradigm will enable us to transform public-private partnerships into public-private joint action, and information sharing into information enabling – timely, relevant, and actionable. Together, government at all levels, industry, and our international allies – because cybersecurity does not begin or end at our borders – will bring to bear our collective capabilities to sustainably shift the balance of power in favor of cyber defenders. We will plan together, exercise together, and act in unison to address both immediate threats and overcome longer-term strategic and systemic cybersecurity challenges. Ultimately, we envision that this integrated public-private collaboration will drive the collective defense of cyber space to create a secure and resilient cyber ecosystem for all Americans, and we look forward to expanding this operational collaboration going forward.

Election security also remains a top priority for CISA. As you know, a number of elections concluded just yesterday as part of the 2021 cycle, including prominent gubernatorial races in Virgina and New Jersey. In support of our election security efforts, CISA hosted an Election Operations Room at our Arlington Office, and virtually around the country, to present an integrated Federal coordination point for support to State and local election officials holding elections this cycle. Partners from the interagency and the election community collaborated in real-time to share information about election risks and be prepared to respond as needed. In

addition, I recently announced that Secretary of State Kim Wyman will be joining CISA as our new Election Security Lead. Kim has recently been the Secretary of State in Washington, and she is joining to help ensure that we have a senior member of the Election community guiding our efforts to address a range of threats to America's democratic process to include cyber and physical threats, as well as mis- and dis-information. I am extremely excited to welcome Kim to CISA.

Another area I want to highlight is CISA's ongoing work to implement the May 12, 2021, Executive Order 14028, *Improving the Nation's Cybersecurity* signed by President Biden. 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 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 or supporting over 35 unique efforts, many with short timelines highlighting the 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;
- Advancing the adoption of leading security practices necessary to address highly adaptive adversaries in collaboration with OMB and other federal partners, including publication of a Secure Cloud Technical Reference Architecture and a Zero-Trust Maturity Model;
- Raising the bar for incident response by publishing a Vulnerability and Incident Response Playbook to federal agencies, which will ensure that all agencies will operate from the same sheet of music during incidents, and enable a coordinated 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 by government contractors, in response to incidents. Such sharing will include the federal agency holding the contract, as well as with CISA. The recommendations to the FAR also establish 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 working with OMB to direct 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.

Building on the Executive Order, this summer, the President also issued a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. The reality is that cybersecurity needs vary among critical infrastructure sectors, but we cannot evolve our Nation's cybersecurity posture without baseline cybersecurity goals that are consistent across all sectors. Additionally, there is also a need for security controls for select critical infrastructure that is dependent on control systems. Working in partnership with the National Institute of Standards and Technology (NIST), at the end of last month, we issued the preliminary cybersecurity performance goals based on nine categories of best practices. These goals are part of a whole-of-government effort to meet the scale and severity of the cybersecurity threats facing our country. Our safety and security rely on the resilience of the companies that provide essential services such as power, water, and transportation and these performance goals should be the standard cybersecurity practices and postures that the American people can trust and should expect for such essential services. It takes all of us committed to action, and that requires harnessing the power of operational collaboration.

Our successes would not be possible without the outstanding and dedicated CISA workforce. For me, it is all about the people - we will be successful because of our people. While I am committed to working to attract and retain world-class talent, one of my top priorities is also to build a workforce that looks like America and has the skills needed to meet the threats of the future. To that end, I am very proud that, in addition to DHS's collaboration with the Girl Scouts of the USA, CISA recently announced a partnership with Girls Who Code, with the intent of closing the gender gap in cybersecurity and developing pathways for young women to pursue careers in cybersecurity and technology. Partnering with Girls Who Code will provide real solutions to tackle diversity disparities and bring together a stronger community of women in technology and cyber. CISA and Girls Who Code will work hand-in-hand to improve the awareness of these careers in cyber, while building tangible pathways for young women, especially young women of color, to get hands-on experience and find opportunities – whether in the private sector, non-profit sector, or part of government.

**Conclusion**

Our nation faces unprecedented risk from cyber attacks undertaken by both nation-state adversaries and criminals, 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.