Testimony of

Christopher C. Krebs

Before the

Committee on Homeland Security

U.S. House of Representatives

On

Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience

February 10, 2021

Washington, DC

Via Cisco Webex

Testimony of Christopher C. Krebs
U.S. House of Representatives, Committee on Homeland Security
February 10, 2021

Introduction

Chairman Thompson, Ranking Member Katko, Members of the Committee, my name is Chris Krebs, and it is my pleasure to appear before you today to discuss "Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience." As you know, I previously served as the first Director of the Cybersecurity and Infrastructure Security Agency (CISA), leading CISA and its predecessor organization, the National Protection and Programs Directorate, from August 2017 until November 2020. Over the last several years, I have had the pleasure of working with many of you as members of the primary oversight Committee for CISA and have testified in front of this committee many times. To the new members of the committee, congratulations on being given the honor to represent your constituents in the 117th Congress. I look forward to working with you.

It is an honor to appear before this Committee to testify about the current cybersecurity threat landscape and how it intersects with American businesses and government agencies. Given my recent experience as CISA Director, and now as Founding Partner of the Krebs Stamos Group, a cybersecurity risk management consultancy, as well as the Newmark Senior Cyber Fellow at the Aspen Institute, I am continuing my efforts to improve the Nation's cybersecurity and resilience. My time at CISA most acutely helped shape my view of the effectiveness of our current approach and its shortcomings, particularly with a focus on critical infrastructure. Operating from an assumption that our adversaries are technically capable, both opportunistic and highly targeted, yet bound by the laws of physics and the realities of the Gregorian calendar, I firmly believe that we can make progress in defending our cybersecurity.

In order to make progress, I believe there are several truisms that are useful to framing an organization's approach to cybersecurity and resilience: First, the federal government is not going to save you, but they are an essential partner. Second, cybersecurity competency requires leadership buy-in. Third, good guys and bad guys alike make mistakes, how fast you find both makes a difference. Fourth, your mistakes are likely going to get out anyway, the faster you protect your customers, the better off everyone will be. And fifth, everyone has bad days, preparation will determine how bad that day is. These truisms represent a simple acknowledgement that 100% security is not the desired or realistic end state, instead a resilient organization that is empowered, informed, humble, and agile can not just survive in today's environment, but actually thrive.

In my testimony today, I will provide a series of recommendations to improve our approach to making the Internet a safer and more secure place for all Americans. These recommendations are rooted in the need to continually improve our understanding of our nation's physical and digital infrastructure, introduce friction into the adversaries' activities, and increase investments and centralized services for government and industry alike. My recommendations align with the more defensive actions associated with "Deterrence by Denial."

1) Continue to invest in CISA's National Critical Functions (NCFs) Initiative, improve our understanding of the risk facing our Nation's infrastructure, and expand roll out to highest risk functions.
2) Prioritize identification of systemically important enterprise software and services, update federal contracting for greater transparency and sharing, and launch operational defensive partnerships called for in the 2021 National Defense Authorization Act.
3) Launch a national countering ransomware initiative to improve defenses, disrupt the ransomware business model, and use broader set of authorities against actors.
4) Proceed with Department of Commerce rulemaking on Executive Order 13984, "*Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*" to counter adversary abuse of Virtual Private Servers.
5) Improve Federal cybersecurity posture through enhanced governance, increased funding, and centralized services offered by CISA.

Understanding Cyber Risk

When thinking about the cybersecurity risks we face today, I find the traditional risk formula most useful to organize the various players on the field:

r=t*v*c

Where r = risk, t = threat, v = vulnerability, and c = consequence. Likelihood of an attack is assumed within the t variable.

Those three variables combined yield the risk we are constantly trying to manage. The three variables, however, are not static nor are they singular, and therefore a risk manager's job is never done. The cyber implications of COVID-19 are a useful case study. In the spring of 2020, our nation's critical infrastructure risk shifted dramatically. The coronavirus spread across the country sickening many Americans and overwhelming hospitals, particularly in New York City. The consequences of a threat – non-state actor ransomware – hitting a hospital would lead to loss of life due to reduced capacity in patient care. To manage the risk in the calculation, through CISA's "Project Taken" we engaged to both minimize vulnerabilities in patient care facilities, but also by messaging threat actors to avoid attacking those facilities. There were also state actor threats from China and Russia conducting espionage on vaccine manufacturing research labs. Those intrusions, exploiting vulnerabilities in the networks and systems of the labs, if conducted recklessly, could result in disruptive consequences to vaccine development, where days and weeks delay in vaccine roll out meant real lives lost. In part, through Operation Warp Speed, CISA worked with vaccine developers to minimize vulnerabilities by sharing threat intelligence, investigate suspicious activity, and scanning for unpatched systems. We also worked to better understand supply chains and manage consequences by identifying and diversifying or hardening single points of failure in the chain from research and development to shots in the arm.

Both real-life scenarios offer just a glimpse into the challenges facing information security teams and risk managers in general across the country. They also highlight the focus cannot solely be on understanding and stopping the threat actors – we must also invest in our ability to understand why we might be targeted by threat actors, how they might come at us, and if they do, how do we survive or minimize any attack.

The T(hreat) Variable

The cyber threat landscape is more complicated than ever, with state and non-state actors investing in and building capabilities that enable everything from run-of-the-mill cybercrime, information operations, destructive attacks, and operations with kinetic affects. Over the last few years, the "state actor cyber club" has evolved from the traditional big four of cyber adversaries - China, Russia, Iran, and North Korea – to a more stratified set of actors. The sorting is based on capability, with China and Russia at the top of the pyramid, and Iran and North Korea, while still capable, a rung below. Non-state actors including cybercriminals are also gaining ground.

Further complicating the ability to paint a clear picture of the cyber threat actor landscape is the increasingly blurring line between state and non-state actors. For example, contracted or proxy cyber actors support or act on behalf of state-directed operations. Conversely, state actors sometimes moonlight as cybercriminals after-hours to earn additional income. And in other cases, non-state cyber actors operate with the tacit approval of the home state, if the actors do not target their own domestic organizations, in other words "anyone but us." New actors enter and leave the playing field daily. Agencies reorganize, break up, and consolidate. Criminal gangs are busted, go dark, or give up the life of crime. If the tools are available, money and secrets are to be had, vulnerabilities exist, and a lack of meaningful consequences persist, there will be malicious cyber actors.

Case Study: Same Nation, Different Tactics

Cyber actors use various techniques, from opportunistic and commonly available, to highly sophisticated and only available to those with resources and time. We saw both play out last year. The Russian FSB, the main successor to the Soviet-era KGB, carried out a broad campaign scanning for unpatched network access points known as VPNs in a variety of sectors, from Federal, state, and local government, to the aviation sector and the defense industrial base. There was nothing particularly sophisticated about this activity, they simply looked for the out-of-date VPNs and exploited them with common techniques. At the same time, the Russian SVR, the main foreign intelligence service, launched a stealthy campaign in late 2019 that used a variety of techniques exploiting trust – the that keeps networks going the world round. They moved downstream from Texas-based information technology (IT) company SolarWinds into customer networks, while also exploiting authentication techniques to gain access to email systems. As we were chasing the noisy FSB (and other actors, like the Iranians and ransomware crews) around the country, the ghostlike SVR was lost in the noise, patiently moving through a select list of targets. And that is just two actor sets from two agencies within one foreign adversary. Each agency has multiple groups, each nation has multiple agencies. Each group, agency, and nation have different strategic objectives and tactics to achieve them.

Unfortunately, across the full set of actors, there is no authoritative perfect picture or master list of the agencies and their tradecraft, tools, personnel, or targeting lists. Instead, we have a modern-day parable of the "Blind Men and the Elephant," where different defenders have a unique perspective based on their viewpoint from where they sit across American infrastructure or from their incident response investigations. This leads to a confusing mashup of threat actor names, be they pandas, APTs, or Periodic Table elements. And that is just from the cybersecurity vendor community. Inside

government and across allied partners there are myriad codenames and jargon for the cyber actors knocking on our networks every day.

The Challenge of Securing Domestic Infrastructure

Our critical infrastructure is what drives our economy, supports national security, and contributes to public health and safety. Most critical infrastructure in the U.S., however, is owned and operated by the private sector with only a patchwork of security oversight in place. It is hard to overstate the massive scope of the critical infrastructure security and resilience challenge. The levers government has at its disposal to change behaviors, on the other hand, is underwhelmingly small.

This leads to three conditions limiting the ability of government and industry to collectively improve critical infrastructure cybersecurity: (1) lack of a deep understanding of what is truly systemically important across the economy, (2) a need for more meaningful methods for operational engagement with industry to address risk; and (3) insufficient funding and investment in security improvements.

Understanding Risk

The first challenge to overcome in enhancing the cybersecurity of our nation's infrastructure is our understanding systemic importance must improve. Even within classic infrastructure sectors and systems that are generally easy to define – banking and finance, energy, and transportation – only now are we really identifying the highest risk functions within those sectors. Fortunately, the effort to understand systemic importance of industry functions is a growing area of focus for the Federal government, in part driven by CISA's National Risk Management Center through the National Critical Functions (NCF) initiative[1]. By gaining a deeper understanding of the critical functions and systems that drive our nation's economy the government can bring together key players to operationalize risk management partnerships and make measurable progress towards a more resilient economy.

NCFs In Practice: Defending the 2020 Election

The concept of organizing around a key NCF was central to the success of the protection of the 2020 election. Led by CISA, the election security community across government and industry came together to understand the greatest risks to the administration of the election, developed strategies and plans to improve security of the key subfunctions and successfully defended the election. We must repeat that intensity of effort across the rest of the NCF set. The NCF initiative, as shown in the defense of the 2020 elections, has already laid the groundwork for the Continuity of the Economy recommendation in the 2020 Cyberspace Solarium Commission (CSC) report, subsequently included in the 2021 National Defense Authorization Act.

One of the most critical aspects of the NCF work will be to support efforts to understand the prevalence of more intangible sectors like information technology and communications. The IT sector is a horizontal or enabling sector rather than a vertical sector. The products and services offered by the IT sector, like computer operating systems, network management software, and cloud computing, are core

[1] National Critical Functions | CISA

to nearly every aspect of the economy – even our Nation's agriculture sector increasingly relies on automated technology to improve efficiency and increase capacity.

To more broadly understand systemic importance of enterprise software and platforms, government and industry must work together to map the key components and players of our nation's IT and communications infrastructure. Of particular focus should be those companies that have a dominant position in their market segment, and any disruption or compromise would have cascading and outsized impacts on the ecosystem. As a byproduct of enjoying economic success, those companies should recognize they have broader corporate citizenship responsibilities and must dedicate resources, personnel, and expertise to protect the very economy they so richly benefit from. At a minimum, companies should reexamine and ensure their approach to securing their products, processes, and customers.

Improving Engagement between Government and Industry

In addition to improving our understanding of infrastructure, we must improve the methods by which we collectively engage on risk management efforts. CISA can lead this important endeavor. The Agency supported the President's National Security Telecommunications Advisory Committee (NSTAC) in developing the 2014 Report to the President on Information and Communications Technology (ICT) Mobilization[2]. The core concept of the report was to develop a working partnership between industry and government that could be immediately activated in the event of a large-scale cyber-attack approaching a National emergency, yet many of the lessons of the report equally apply to steady state resilience building activities. Two recommendations emerged from the report that are even more important than they were just a half decade ago.

1) **Conducting a Unified Risk Assessment**: The first is tighter integration between the collectors and analyzers from industry and government of foreign cyber actor intelligence, in part through a Unified Risk Assessment Process for Mobilization. This fusion of private and public intelligence expertise can overcome the current imperfect nature of understanding, decision-making, and response. A unified risk assessment process in both steady state and response scenarios would bring together informed and experienced hands to determine means, intent, and ability to understand a potential or ongoing threat actor campaign. Most importantly, the private sector and civilian agency experts can bring context and relevance to intelligence analysts that may not have a sufficient understanding of the domestic infrastructure landscape, which can lead to overlooking the relevance of collected intelligence. This risk assessment process and the contributing analysts should be a core function of the Integrated Cyber Center recommended by the Cyberspace Solarium Commission (Recommendation 5.3) and included in the 2021 NDAA, Section 1731 (Establishment of an Integrated Cybersecurity Center). The concept also echoes the recommendation of the President's National Infrastructure Advisory Council (NIAC) for the establishment of a Critical Infrastructure Command Center (CICC)[3].

[2] NSTAC - Information and Communications Technology Mobilization Report 11-19-2014.pdf (cisa.gov)
[3] https://www.cisa.gov/sites/default/files/cisa/NIAC Actionable Cyber Intelligence_DRAFT-PREDECISONAL_508c (002).pdf

2) **Establishing a ICT Enablers Working Group**: The 2014 NSTAC report also "developed a working model of the functional capabilities (in six categories) associated with the broader global ecosystem[4]." The companies that execute these capabilities are known as "ICT Enablers." While the core functions of the ICT Enablers no doubt require a fresh look and update, the purpose is the same – we must understand the core functions and the companies that substantially make up those functions. This is the essence of systemic importance in the IT Sector, those companies that dominate or hold a lynchpin position in the ecosystem have an outsized responsibility to contribute to the national defense. We must know who these companies are and then establish meaningful partnerships between industry and government. Not just to trade business cards, but to share information on emerging threats or observed attacks.

Through the knowledge transfer associated with trusted partnerships, combined with the commitment and support of corporate leadership, the baseline of security across the ICT enablers should improve. Prior models have fallen short principally due to a lack of specificity in tasks and the inability of government to host industry representatives outside of a handful of Information Sharing and Center (ISAC) representatives. By adopting a risk management agenda with discrete tasks and skillsets required, and industry organizing itself with deliberate representation of the companies that truly matter, much like the United Kingdom's National Cyber Security Centre Industry 100 model, CISA can more effectively identify and work with industry partners. The entity resulting from the Integrated Cyber Center or CICC mentioned above, building on existing CISA coordination mechanisms, can bring government and industry together to improve partnership models to operationalize intelligence and risk management efforts.

Increasing Funding for States and Incentivizing Industry Investment

Even by identifying our infrastructure of concern and creating the mechanisms for engagement, it requires resources to secure systems, hire and train personnel, and engage in collective efforts. For state and local government partners, even if awareness is not an issue, lack of funding is an ever-present inhibitor to improving security.

1. **State and Local Cyber Grants**: Congress should identify grant programs, much like the Homeland Security Grant Program, to distribute funding to state and municipal infrastructure programs to help improve their security programs. Grant programs should incentivize regional collaboration and coordination, creating a mutually supporting culture and community of security.
2. **Expanding Training to Government Infrastructure**: CISA should also be authorized and funded to provide entry and mid-level information security and operational security education and training programs. These programs should prioritize remote learning opportunities in order to engage more students, but where more advanced or hands-on learning is more effective, CISA should be funded for mobile training capabilities to bring training to the students where they are.
3) **Industry Incentives**: Industry should similarly be encouraged to invest in security programs, ideally through sector self-organization and implementation. In the meantime, the Executive

[4] NSTAC Report to the President on Information and Communications Technology Mobilization, pg 14.

branch should conduct a meaningful review of existing regulatory programs for cybersecurity requirements or extant authorities that could be used to require additional security. We are also seeing a emerging class of corporate leaders that understand the importance of cybersecurity and the need to invest. Conversely, there will always be a set of executives that look to shave costs and minimize outlay until forced to spend, if even then. With the appropriate engagement and education, the former class – particularly when identified as systemically important and provided the opportunity to best improve the security of their operations – should outpace the latter. After a period of time, all executives may prefer a more prescriptive approach with certainty.

4) **Government Contracting Requirements**: The government should start with where it does business with industry, government should require standardized security practices as a matter of contracting. The U.S. government can immediately improve visibility and understanding across Federal networks (though there will be cascading benefits to industry) by amending the contracting process to require transparency about the software itself, the level of access the software requires to operate, and the security measures in place to ensure the software cannot be manipulated through development, build, installation, operation, or maintenance. In addition, CISA should be included in the contract as an authorized recipient of vulnerability and incident notifications. As of now, privity of contract and the bounds of Non-Disclosure Agreements (NDAs) limit the sharing of information on risks or incidents beyond the vendor and the customer. This puts the vendor in the position of not being able to share information with CISA for broader understanding of an emerging or ongoing incident.

The Growing Ransomware National Emergency

Today's cyber threat landscape is not monopolized by state actors, in fact, the threat that most immediately and measurably affects the average American is cybercrime. Ransomware, specifically, has been on a steady rise over the last several years, with ransomware gangs typically operating out of countries that turn a blind eye toward their crimes, as long as the victims are foreign, and the money comes back home. According to the 2020 Verizon Data Breach Report, Ransomware accounts for 27% of malware incidents, with the highest rate of occurrence in the education, healthcare, and government administration sectors[5]. Ransomware crews have been propelled and professionalized by commodity malware and specialization across various hacking techniques, but also thanks to the availability of cryptocurrencies that allow for anonymous financial transactions.

The U.S. along with our allies need to take a new, more strategic and coordinated approach to overcoming the emerging national security emergency posed by ransomware. The counter ransomware "triplet" includes improving cyber defenses, disrupting the criminals' business model, and increased coordinated action against ransomware gangs and their enablers. This strategy will require government and the private sector to contribute and commit to partnering together to break the ransomware cycle.

Improving Defenses

[5] 2021 Verizon Data Breach Report, Figure 5., pg 7. Available for download here.

First, we must improve defenses of our businesses and agencies across all levels of government. Ubiquitous use of multifactor authentication (MFA) for access to networks can limit credential abuse, updated and patched systems can prevent actors from exploiting known vulnerabilities, and a well-practiced incident response plan accompanied by backed up and offline systems can enable rapid reaction and restoration. In many cases, even these straightforward steps are beyond the reach of many companies or state or local agencies. We need to rethink both our approach to technology deployment, including MFA by default, and the Federal government should consider increasing technology upgrade grants to states and localities to retire legacy systems and join the digital transformation. The return on investment will extend beyond increased security and improve the efficiency of citizen services, support the U.S. technology sector, and open up more skilled technology jobs for a sluggish American workforce.

Disrupting the Ransomware Business Model

Second, we must break the business model of ransomware. Simply put, ransomware is a business, and business is good. The criminals do the crimes and their victims pay the ransom. Often it is easier to pay and get the decryption key than rebuild the network. There are three problems with this logic: (1) you are doing business with a criminal and expecting them to live up to their side of the bargain. It is not unusual for the decryption key to not work. (2) There is no honor amongst thieves and no guarantee that the actor will not remain embedded in the victim's network for a return visit later, after all the victim has already painted themselves an easy mark. (3) By paying the ransom, the victim is validating the business model and essentially making a capital contribution to the criminal, allowing them to hire more developers, more customer service, and upgrade delivery infrastructure. And, most worrisome, go on to the next victim. A useful law school exam question may be whether in a string of ransomed companies, if a victim of a subsequent ransomware attack might pursue legal action against a prior victim of the same crew that had paid off the criminal. There is likely no viable course of action here but continuing to allow for ransom payments is a net public policy negative.

We must address the ransomware business model head on and disrupt the ability of victims to pay ransom. First, cryptocurrencies should be either more heavily regulated or provide for more transparency via Know Your Customer regimes for cryptocurrency exchanges. Second, we need a national policy conversation on whether payments should be lawful. The Office of Foreign Asset Control (OFAC) has already started this dialog, declaring ransom payments to identified entities may be a violation of economic sanctions laws. Because the identity of the ransomware actor is not always obvious, the OFAC advisory may have an overall chilling effect on ransom payments.

More Aggressive Action Against Ransomware Actors

Third, we need more coordinated action against ransomware actors using the range of authorities available to federal agencies, as well as capabilities and rights resident in the private sector. To be perfectly clear, I am not suggesting extrajudicial kinetic actions against ransomware gangs. However, other authorities available to law enforcement and military should be on the table, with great care taken not to blur the lines between the two. Traditional approaches have clearly not been sufficient to prevent the outbreak of ransomware. More aggressive disruption of malware command and control

infrastructure, like the recent action against *Emotet*, is a good start[6]. Where there are clear ties between ransomware actors and state actors or a potential imminent threat to an event or infrastructure of significance like a national election, action should be on the table. The private sector also has options available, as demonstrated by Microsoft's aggressive policing the abuse of its trademark and source code, including last fall's operation against *Trickbot*[7]. When coordinated and jointly conducted, private and public sector can make the internet an inhospitable place for cybercriminals. The recent establishment of the National Ransomware Task Force, hosted by the Institute of Security and Technology[8], is a promising private sector collaboration to change the rules of the game, assuming strong engagement and coordinated action with the Federal government.

Adversary Abuse of Infrastructure as a Service

Much of the state and non-state actor cyber activity targeting U.S. businesses and agencies uses our very own technology against us. State and non-state actors alike are using cloud infrastructure services and the protections afforded by law and the Constitution to steal intellectual property and potentially position themselves for future attacks. According to Ambassador Robert O'Brien, President Trump's last National Security Advisor, "(m)align actor abuse of United States (Infrastructure as a Service) products has played a role in every cyber incident during the last four years.[9]" To stem the abuse of IaaS products, the last Administration signed out Executive Order 13984, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities.[10]" The EO directs the Department of Commerce to release for notice and comment regulations within 180 days that describe a regime that would require cloud service providers to implement "Know Your Customer" and Suspicious Activity Reporting measures.

While the new administration is obviously within its rights to review and revise or withdraw any pending rulemaking, this regulation, with adequate input from industry and cloud users, can limit abuse of cloud services through increased transparency. Even in the absence of the regulation, it would be wise for industry to consider adopting a voluntary set of transparent practices that would achieve the same outcome, absent Federal government intervention.

Improving Federal Civilian Agency Cybersecurity

As demonstrated by recent Russian intelligence activities, Federal agencies remain at the top of the targeting list for foreign cyber actors. Our nation's 101 Departments and Agencies civilian agencies hold a wealth of unclassified information across a vast assortment of unevenly secured, monitored, and even mapped networks and systems. Despite an increased availability and deployment of cybersecurity tools via the National Cyber Protection System and the Continuous Diagnostics and Mitigation (CDM) program over the last six years, more must be done. Other shifts and gaps in the federal government IT space have hampered the ability of agencies to keep pace with the threat landscape. At the macro-level,

[6] Emotet Botnet Disrupted in International Cyber Operation | OPA | Department of Justice
[7] New action to combat ransomware ahead of U.S. elections - Microsoft On the Issues
[8] Institute for Security and Technology (IST) » Ransomware Task Force (RTF)
[9] Press Release - Statement from National Security Advisor Robert C. O'Brien | The American Presidency Project (ucsb.edu)
[10] 2021-01714.pdf (govinfo.gov)

there are three general themes that hamper our ability to properly secure the .gov, even after several years and billions of dollars invested in security. First, there is still insufficient funding for modernization and new security tools. Second, there is a need for stronger governance across agencies. And third, visibility into network traffic is eroding due to increased use of encryption (a good thing!) and a shift to cloud-based services (also a good thing, if done properly).

Accelerated Investment in CISA Security Programs

Investing in federal IT is not a one-shot deal, maintaining a modern and secure environment is simply the cost of doing business in today's world. This is particularly true as more and more services go digital and most of the federal workforce remains remote due to COVID (and may remain remote for the foreseeable future). In the face of the these shifts and the attackers' relentless efforts to find seams in our defenses, Congress must not blink, even in the wake of the SolarWinds supply chain compromise.

The CDM program remains the critical core of Federal cybersecurity, though it is not currently deployed broadly or deeply enough in part due to agency ability to deploy at scale quickly, underestimation of required services, and funding constraints. CDM focuses on who and what makes up the network, including assets, identity, and data. Recently, NDAA Section 1705 authorized CISA to conduct proactive threat hunting across civilian networks, a key development in improving visibility across the 101 agencies. For this advancement to be successful, CISA will need to deploy detection capabilities, hire analysts to conduct the activities, gain access to the appropriate data, and the buy-in and cooperation from the agencies CISA is hunting across. With accelerated capability coverage and additional Federal agency support through expanded financial resources, CDM will more effectively and efficiently serve Federal agencies to search for and where necessary remediate Russian actor intrusions. CDM can also serve as a force for change and modernization across the Federal government. Last spring, as COVID sprung up and threat actors targeted Health and Human Services networks, the program rapidly responded to help HHS upgrade security and systems to protect pandemic response and research. can be a catalyst for continued IT and cyber modernization across the Federal enterprise.

Stronger Governance Across Federal Civilian Agency Networks

At the governance level, roles and responsibilities across the Federal government are unclear, potentially further complicated by the newly authorized National Cyber Director (NCD) created by Section 1752 of the NDAA. Regardless of the organizational structure, the Executive branch must establish a comprehensive strategy and vision for Federal network modernization and security, drawing in the Budget side of the Office of Management and Budget (OMB) to coordinate and consolidate budgetary oversight, the Federal CISO as the policy framer, CISA as the tool provider and enforcer of security policy. The respective roles and responsibilities of the Federal CISO and CISA should also be examined. In effect, CISA is serving as the operational CISO for the federal government, particularly with the recent NDAA authorities – this position should be strengthened. Federal agencies are of course a part of this effort, but as time and our adversaries have proven, there are currently not enough technical resources and personnel available at the individual agency level to meaningfully protect the .gov in 101 different instantiations. Therefore, the Federal government must set very clear cybersecurity expectations and standards for agencies and Congress should fund those expectations. There should be two paths for agencies to choose: (1) you either meet the enhanced standards set out or (2) CISA can do it for you. The

first option, while achievable and likely appealing to agencies mature and confident in their ability to manage their enterprise risk, will also require funding unavailable to most agencies. Even then, it is economically inefficient for even the most mature agencies if a comparable offering exists elsewhere.

Increasing Visibility Through Centralized Services

The second option plays into the third area for improvement, increased visibility through centrally managed services. The NDAA threat hunting authorities provided to CISA will provide increased visibility at the host level, however, there are additional visibility gaps that need to be addressed. For example, as agencies have shifted to cloud-based services – particularly during the pandemic – CISA lost visibility into network traffic. That decrease in visibility is in part due to increased encrypted traffic, but also because the entire point of modern cloud-based "Workplace as a Service" is for the user to interact directly with the cloud rather back to the agency's network via a trusted connection. To do this securely, however, requires consistency and discipline in implementing the appropriate security controls, as well as collecting and maintaining the forensic records to empower detection, analysis, and response. To ensure consistency and appropriate logging, CISA should work with OMB and GSA to create a customer-centric, security-first hardened cloud-based email environment. This approach would be economically sensible at the macro and micro levels and would be centrally defensible to adversary attacks.

Even this may be too permissive of an arrangement and only a half-step towards the most logically defensible arrangement for civilian agencies – a centrally managed and secured "Govnet." Common services that touch the public internet, including email, should be consolidated as much as possible, ideally by CISA's Quality Service Management Office (QSMO)[11]. Such a configuration would clearly be an attractive target to attackers, and yet by consolidating security teams, visibility, and ability to act, a more resilient infrastructure is possible.

Conclusion

The piece parts are in place for our nation to dramatically improve our cybersecurity defenses. We need to as a society accept that that, yes, each and every organization in the country whether private sector or government, can be targeted by a cyber actor. And no, the government is not going to save you. And yes, there is something that you can do about it, in fact you have a responsibility to your customers, stakeholders, and depending on where you sit in the economy, a responsibility to the country.

The key ingredients needed are leadership awareness and commitment in the private sector and a bolder vision from government. That alone will not immediately solve the problem, but with those two pieces folded together, investment will follow, defenses will improve, and organizational and economic resilience will increase. It will take time and we will never reach or even see a finish line. Cybersecurity is an ever-evolving discipline, and the threat actors are motivated by a variety of incentives that we may never fully comprehend. But change for the better is possible, we just need to stop waiting for it to happen to us and instead, to quote Mahatma Ghandi, "be the change we wish to see in the world."

[11] Cyber QSMO Marketplace | CISA

Thank you not only for this opportunity to testify before the Committee today on this critical issue, but also for your partnership over the last several years. I have no doubt that my successor will enjoy a productive working relationship with the Committee and that together we can continue to improve the Nation's cybersecurity and resilience.

I look forward to answering any questions you might have.