Testimony

Eric Goldstein

Executive Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

Committee on Oversight and Reform

Subcommittee on National Security

July 27, 2021

Washington, D.C.

Chairman Lynch, Ranking Member Grothman, and members of the subcommittee, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding the Biden Administration's efforts to secure the nation's electric grid from cyber-attacks, and to discuss whether additional authorities and deeper public-private partnerships are needed to address vulnerabilities in U.S. bulk power and electric distribution systems.

CISA leads the Nation's efforts to advance the cybersecurity, physical security, and resilience of our critical infrastructure. In particular, CISA serves as the focal point to exchange cyber defense information and enable operational collaboration among the Federal Government, SLTT Governments, the private sector, and international partners. In this role, we are particularly focused on reducing cybersecurity risks to entities that provide or support National Critical Functions, which includes public power utilities.

To accomplish this mission, CISA leads a collaborative effort to identify and drive reduction of the most significant cyber risks to the nation's critical infrastructure. This requires first identifying cyber risks through robust multi-directional information sharing, conducting risk and vulnerability assessments, and deploying threat detection technologies to critical assets. We work to prioritize identified risks, including by leveraging the capabilities of our National Risk Management Center to understand relative criticality of critical infrastructure assets and working with our partners across government to understand our adversaries' potential intent and capabilities. Finally, we drive collective action to reduce cybersecurity risks, including by providing incident response and threat hunting services, issuing alerts and guidance, and coordinating joint cyber defense operations that bring together capabilities from government and private sector partners.

Cyber intrusions over the past several months have highlighted that our country is facing an immediate threat to our national security, economic prosperity, and public health and safety. Nation-state actors and criminal groups continue to increase in their sophistication and in their willingness to target organizations across all sectors of the economy. The impacts of these attacks is becoming more severe, impacting the provision of critical functions from healthcare to energy to agriculture. This hearing provides a timely opportunity to emphasize the urgency of this challenge, discuss CISA's critical role in helping our nation manage this risk, and consider necessary steps to drive further progress.

Managing a Broader Risk: CISA's Role in the Nation's Electricity Sector Cybersecurity

In today's rapidly changing world, our Nation's electricity infrastructure continues to face new threats and challenges, many of which require an integrated risk management approach and close coordination between the government and private sector to address. CISA has a longstanding relationship of cooperation and collaboration with the electricity sector, in close partnership with DOE as the Sector Risk Management Agency for the energy sector, that we are keen to strengthen and evolve given the serious cybersecurity threats this vital sector faces every day. CISA understands that securing our nation's electricity sector is a vast and complex endeavor. Many of the necessities of modern society, from putting food on our tables to keeping lights on in our homes, depend on the reliability of our communications and power networks, and the devices that control them. As these systems become more complex, critical equipment is increasingly connected digitally making these systems more efficient, but also more susceptible to intrusions by our adversaries. Attacks on operational systems not only endanger the American way of life but threaten to directly take lives. CISA is working with the companies that power America to ensure that their efforts to serve customers in new ways are designed with security principles fit for the 21st Century.

Over the years, we have seen the electricity subsector's owners and operators place a greater emphasis on secure software development, as well as acquisition processes and practices that consider network security. The electricity subsector has also been involved in cyber exercise planning workshops and seminars designed to assist organizations at all levels in the development and testing of cybersecurity detection, protection, and response capabilities.

For example, the North American Electric Reliability Corporation (NERC) hosts a Grid Security Exercise (GridEx) every two years, and it is an outstanding example of our strong public-private partnership. Through CISA's participation in GridEx, we have witnessed utility companies demonstrate how they would respond to and recover from cyber and physical security threats and incidents, strengthen their crisis communications relationships, and provide input for lessons learned.

Over the last decade, our relationship with the electricity subsector has evolved into a valuable and increasingly trusted partnership. CISA's primary goal is to help those that own and operate our Nation's infrastructure identify, analyze, prioritize, and manage the risks they face. The following examples showcase our shared commitment and progress to providing the electricity services essential to Americans' lives.

First, DOE and CISA worked closely with the electricity subsector after a December 23, 2015, campaign led by Russian government cyber actors that caused outages to three Ukrainian power companies, leaving nearly a quarter-million customers without power. We partnered with the Electricity Information Sharing and Analysis Center (E-ISAC), which was stood up in 1999 to offer security services to owner and operator organizations of the Bulk Power System across North America. Our incident response capaibility sent a team to Ukraine to help the impacted entities recover from the attack and implement mitigation techniques.

Second, in 2018 we formalized effective energy sector partnership mechanisms, including the Tri-Sector Executive Working Group and with the E-ISAC. The Tri-Sector Executive Working Group was chartered under the Critical Infrastructure Partnership Advisory Council (CIPAC) with representatives with the financial services, electricity subsector and communication sectors. This working group is designed to facilitate and integrate a collaborative approach to risk management and address sector-specific capability gaps, cross-sector strategic challenges, and resilience during significant events affecting critical infrastructure. The long-term goal of the working group is to serve as a model for strategic coordination and establish a framework for operational collaboration that can be expanded to other critical infrastructure sectors. The E-ISAC is an example of how utility interests are working to secure their infrastructure across the sector. The E-ISAC regularly collaborates with CISA and the

Department of Energy (DOE) to provide its members and partners with resources to reduce risk. Two-way sharing of information on cyber threats and vulnerabilities between the private and public sector will enable us to enhance network defenses and deny benefits to our adversaries.

Third, in April 2019, CISA published an initial set of 55 National Critical Functions (NCFs), which are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfuntion would have a debilitating effect on security, the economy, or public health or safety. Several of these National Critical Functions are directly related to the electricity sector because many industries depend on the electric grid. CISA continues to work with government and industry partners to identify and manage risks to the NCFs in a targeted, prioritized, and strategic manner to improve resilience across the Nation's critical infrastructure

Fourth, on April 20, 2021 DOE, CISA, and members of the electricity sector kicked-off an initiative to enhance the cybersecurity of electric utilities' industrial control systems (ICS) and secure the energy sector supply chain. The Biden Administration's "Industrial Control Systems Cybersecurity Initiative" and "Electricity Subsector 100-Day Action Plan" are a coordinated effort that represents rapid, aggressive actions to confront cyber threats from adversaries who seek to compromise critical systems that are indispensable to U.S. national and economic security. While this joint initiative is still ongoing, this partnership with the DOE and the electricity subsector participants will create deeper cross-sector expertise that will better protect the U.S. electric system, while providing a valuable pilot to secure industrial control systems across all critical infrastructure sectors.

Ransomware: A Growing Threat

Ransomware is an ever-evolving form of malware that encrypts files on a device, rendering the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption, and often threaten to sell or leak the victim's data if the ransom is not paid. Malicious actors continue to evolve their ransomware tactics over time, and CISA remains vigilant of ransomware attacks and associated tactics, techniques, and procedures across the country and around the world.

Recently, ransomware attacks have surged among state, local, tribal, and territorial (SLTT) governments and critical infrastructure organizations. In fact, it is estimated that over 100 federal, state and municipal agencies, over 500 medical centers, and 1,680 educational institutions in the United States were hit by ransomware in 2020 and ransom demands exceeded $1 billion dollars.[1] This epidemic is now affecting our nation's most critical infrastructure: municipal governments, police departments, hospitals, schools, manufacturing facilities, and of course, pipelines.

CISA, and the Department of Homeland Security, have acted urgently to catalyze national action around this risk. In January 2021, CISA unveiled the Reduce the Risk of Ransomware Campaign to raise awareness and combat this ongoing and evolving threat. The campaign is a focused, coordinated and sustained effort to encourage public and private sector organizations to implement best practices, tools and resources that mitigate ransomware risk. Additionally, in coordination with the Multi-State Information Sharing and Analysis Center (MS-ISAC), CISA released a joint Ransomware Guide that details industry best practices and a response checklist that can serve as a ransomware-specific addendum to state and local government's cyber incident response plans.

In February, during his first remarks dedicated to cybersecurity, Secretary Mayorkas issued a call for action to tackle ransomware more effectively. To further drive a call to action, Secretary Mayorkas initiated a Ransomware Sprint in April 2021 that has included a series of high-profile national events intended to ensure that leaders across all sectors of the economy understand the criticality of this risk and take urgent action in response. During the sprint, Secretary Mayorkas also worked with his counterparts in Australia, Canada, New Zealand, and the United Kingdom and issued a joint statement committing to stronger international collaboration to tackle this threat.

On July 15, Secretary Mayorkas also announced the launch of stopransomware.gov , the first whole-of-government one-stop-location website providing guidance and resources on how to better protect and defend against ransomware.

Ransomware is a critical challenge and the risks posed to our nation's critical infrastructure are severe -- one need look no further than the ransomware attack that crippled the Colonial Pipeline Company and roiled the U.S. oil market or the JBS ransomware attack that highlighted the potential vulnerabilities of our food supply chain. While a debilitating attack against our electric grid has not occurred, when considering recent attacks against critical infrastructure, it is not hard to imagine such a scenario. But the challenge is not insurmountable, and by investing in improved cybersecurity as recommended in CISA guidance, organizations can reduce the risk of a ransomware intrusion and limit the potential impacts. Most ransomware attacks generally exploit known security weaknesses or a failure to adopt generally accepted best practices. However, we are seeing a rising trend of more sophisticated attacks that do use zero-day vulnerabilities or exquisite tradecraft, as was the case in the Kaseya VSA compromise. By investing in improved cybersecurity, as recommended in CISA guidance, organizations can reduce the risk of a ransomware intrusion and limit the potential impacts.

Mitigating Risks

The Colonial Pipeline ransomware attack and the more recent intrusion into JBS Foods and Kaseya must serve as an urgent call to action to address our nation's cybersecurity risks. We must collectively and with great urgency strengthen our nation's cyber defenses, invest in new capabilities, and change how we think about cybersecurity, recognizing that all organizations are at risk, and we must focus on assuring the resilience of essential services. To that end, CISA is acting with the utmost resolve to drive reduction of cyber risk across the National Critical Functions. Achieving the progress we seek will require consideration of several key areas.

First, CISA is currently investing in, and growing capabilities to increase, visibility into cybersecurity risks across federal agencies and across non-federal entities. This necessitates a fundamental change, in which CISA must gain the ability to conduct persistent hunts for threat activity, ingest and analyze security data at all levels of the network, and conduct rapid analysis to identify and act upon identified threats. 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. President Biden's Executive Order on *Improving the Nation's Cybersecurity* will drive critical progress in advancing cybersecurity across the federal government. Going forward, we must take lessons learned from our investments in federal cybersecurity to support organizations across sectors in driving similar change.

Second, given the criticality of public power utilities and certain other critical infrastructure assets, CISA offers a pilot program called CyberSentry, which deploys technologies and analytic capabilities to monitor an organization's business (IT) and operational technology/industrial control system (OT/ICS) network for sophisticated threats. CyberSentry is a voluntary partnership with private sector critical infrastructure companies using CISA's unique statutory authorities, policy and privacy solutions. This capability is not a replacement for commercial solutions; rather, the capability complements such solutions by allowing CISA to leverage sensitive threat information. CyberSentry has shown significant benefit in practice and has been used to drive urgent remediation of threats and vulnerabilities. Due to the success of CyberSentry to date, CISA is working to expand this capability to additional critical infrastructure partners.

Third, CISA must continue to invest in and mature our voluntary partnerships with critical infrastructure entities. For example, our Cyber Information Sharing and Collaboration Program (CISCP) serves as a bi-directional forum in which CISA and private industry are collaborating on significant risks, developing sector and threat focused products, and providing briefings on new trends, threats, and capabilities across the sectors. With information sharing protections available through the Cybersecurity Information Sharing Act of 2015 and the Protected Critical Infrastructure Information Act, the program enables trusted sharing between CISA and a network of high impact companies, Information Sharing and Analysis Centers (ISACs), and service providers. Within CISCP, the Mutual Interest Initiative brings together cyber threat companies and internet service providers to work with CISA and the broader government community to exchange analysis and collaboratively work on threat actor focused products. Furthermore, CISCP enables CISA to work in close coordination with software vendors and endpoint detection companies to both assess impact and mitigate risk of critical vulnerabilities. From a technical standpoint, these partnerships with industry enable us to better understand the nature of vulnerabilities pre- and post-disclosure and in turn provided timely and thorough mitigation guidance to government agencies and critical infrastructure. Going forward, CISA is establishing a Joint Cyber Planning Office, as required by the Fiscal Year 2021 National Defense Authorization Act, to further mature our capabilities to plan, exercise, and coordinate cyber defense operations with partners across the government and private sector.

Fourth, CISA must work with all possible partners to gain increased visibility into national risks. With increased visibility, we are able to better identify adversary activity across sectors, which allows us to produce more targeted guidance, and identify particular incidents requiring a specialized CISA response team. We look forward to working with Congress in considering potential incident reporting legislation that would drive further reporting of cybersecurity incidents to CISA, and other designated federal agencies, in order to further enable this essential visibility.

Lastly, recognizing that we cannot prevent all intrusions, we must drive a focus on resilience and functional continuity even as we drive improvements in security. We must advance business continuity exercises even as we catalyze adoption of cybersecurity best practices; we must ensure that operational technologies is segmented from and can run independently from business networks even as we advance our ability to detect threats in both environments; and, we must reduce single points of failure across our National Critical Functions as we identify and harden identified nodes of systemic risk.

Conclusion

Our nation is facing unprecedented risk from cyber attacks undertaken by both nation-state adversaries and criminals. The list of significant incidents in recent months is long and growing. Now is the time to act – and CISA is leading our national call to action. We will deepen our partnerships with critical infrastructure partners, enhance our visibility into national cybersecurity, and drive targeted action to reduce vulnerabilities and detect our adversaries. In collaboration with our government partners, critical infrastructure entities, our international allies, and with the support of Congress, we will make progress in addressing this risk and maintain the availability of critical services to the American people under all conditions.

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