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

Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack

Committee on Homeland Security

Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation

And

Transportation & Maritime Security

June 15, 2021

Washington, D.C.

Chairwoman Clarke, Chairwoman Coleman, Ranking Member Garbarino, Ranking Member Gimenez and members of the Committees, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding the federal response to the Darkside ransomware incident against the Colonial Pipeline company and the broader cyber threat facing our nation's critical infrastructure.

CISA leads the Nation's efforts to advance the cybersecurity, physical security, and resilience of our critical infrastructure. In particular, CISA serves as the nation's "cybersecurity quarterback" and acts as the focal point to exchange cyber defense information and enable operational collaboration among the Federal Government, state, local, tribal, and territorial (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, including companies like Colonial Pipeline.

To accomplish this mission, CISA leads a collaborative effort to identify and drive reduction of the most significant cyber risks to 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 further reflected the fact 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 malicious activities continue to increase, 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.

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 intrusions and associated tactics, techniques, and procedures across the country and around the world.

Recently, ransomware directed at SLTT governments and critical infrastructure organizations has surged. 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 broader Department of Homeland Security, has 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.

Ransomware is a critical challenge and the risks posed to our nation's critical infrastructure are severe. But the challenge is not insurmountable. Ransomware intrusions generally do not use zero-day vulnerabilities or exquisite tradecraft, but rather exploit known security weaknesses or a failure to adopt generally accepted best practices. By investing in improved cybersecurity as recommended in CISA guidance, organizations can reduce the risk of a ransomware intrusion and limit the potential impacts.

An Example of a Broader Risk: Colonial Pipeline Ransomware Intrusion

The ransomware that impacted Colonial Pipeline was one of the first cyber intrusions in our nation to have a direct effect on many Americans' daily lives. But the intrusion itself was not unique: the Darkside ransomware-as-a-service group has been associated with hundreds of intrusions in recent months and ransomware intrusions have impacted essential services on a smaller scale, from elementary schools to hospitals. Upon learning of the intrusion, CISA immediately began to collaborate with the Federal Bureau of Investigation (FBI) and other interagency partners to gather information that could be used to help protect other potential victims. Within four days of the intrusion, CISA and the FBI published a cybersecurity advisory

[1] Emisoft, *The State of Ransomware in the US: Report and Statistics 2020*, https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/; Emisoft, *The Cost of Ransomware in 2020: A Country-by-Country Analysis*, https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/.

on the incident, which included detailed information on how to reduce risk across critical infrastructure. This advisory contained specific mitigation measures to reduce the likelihood of a ransomware intrusion and, critically, steps to reduce the consequences. This latter element cannot be overstated: all critical infrastructure organizations should assume that they can be compromised by a ransomware intrusion and take steps to reduce impacts, including by ensuring that their essential functions can remain operable even if their primary business network is unavailable. CISA and the FBI subsequently enriched this advisory with specific indicators of compromise associated with the Darkside ransomware group and the Colonial Pipeline intrusion.

In order to further amplify the importance of these mitigation steps, CISA convened a broad stakeholder call with over 8,000 attendees from across U.S. critical infrastructure to provide an overview of the incident, threat actor, and impacts. CISA also convened a meeting under its Critical Infrastructure Partnership Advisory Council with leadership from the 16 critical infrastructure sectors to discuss potential operational impacts for critical infrastructure due to the ransomware intrusion. This contributed to CISA's ability to assess potential impact to the 55 National Critical Functions from a sustained shutdown, and anticipate cross sectoral impacts, including from transportation slow-downs and impacts to chemical facilities. Finally, CISA leveraged our regional personnel deployed across the country, and particularly in areas impacted by the Colonial Pipeline outage, to provide focused guidance to other critical infrastructure organizations and provide the U.S. government with detailed information on cascading impacts across sectors.

Managing a Broader Risk: CISA's Role in Pipeline Cybersecurity

Well before the Colonial Pipeline intrusion, CISA was addressing cybersecurity risks to pipelines. Over the past several years, CISA and the Transportation Security Agency (TSA), in conjunction with the Department of Energy, National Laboratories, and private industry, have been focused on addressing cybersecurity risks to the nation's 2.7 million miles of pipeline infrastructure through the Pipeline Cybersecurity Initiative (PCI). The PCI was formed in response to increasing dependence on automation within the oil and natural gas (ONG) pipeline industry and the growing attack surfaces of assets using connected technology.

As part of PCI, CISA collects, aggregates, and analyzes data to inform a holistic view of vulnerabilities, threats, and consequences to the ONG pipeline industry. Importantly, CISA also provides incident response and intelligence support for pipeline activities with a focus on industrial control systems and coordinates activities related to the PCI. In February 2021, CISA released a Pipeline Cybersecurity Resources Library to provide pipeline facilities, companies, and stakeholders with a set of free, voluntary resources to strengthen their cybersecurity posture.

To inform CISA's analysis of pipeline risk, CISA routinely partners with the TSA and pipeline companies to conduct in-depth vulnerability assessments, or Validated Architecture Design Review (VADR) assessments, on their infrastructure. Importantly, VADRs assess pipeline critical infrastructure information technology (IT) and operational technology (OT) systems to determine if they are designed, built, and operated in a reliable and resilient manner. These assessments, which are free to participating companies, help identify gaps across infrastructure operators. TSA and CISA are on track to complete 52 VADRs on pipeline entities by the end of this fiscal year. To build on the VADR assessment recommendations, CISA and TSA are working with the ONG Subsector Coordinating Council (SCC) to analyze VADR findings, conduct follow on analysis, and develop recommendations for pipeline owners to voluntarily implement.

Given the criticality of certain pipeline entities 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.

Separately, in partnership with a National Laboratory, CISA is developing a suite of tools to assess cyber resilience through scenarios using specialized threat models and simulations to identify "crown jewel" components within pipeline OT. Going forward, the PCI is planning a pipeline cyber table-top exercise to better understand the impacts of an OT compromise at a major natural gas transmission line and is collaborating with industry to integrate pipeline considerations into CyberStorm VIII – a CISA-led biennial exercise series that provides the framework for the nation's largest cybersecurity exercise – in Spring 2022. PCI's future efforts will center around determining the prevalence of major components within pipeline OT systems to identify potential vulnerabilities and inform supply chain risk efforts. CISA will continue leveraging CyberSentry and move to expand the entities receiving such services. Lastly, CISA will lead the development of a pilot tool focused on liquid pipelines that will allow users to explore how disruptions to pipelines can have cascading consequences on National Critical Functions.

Mitigating Future Risks

The Colonial Pipeline intrusion and the more recent intrusion into JBS Foods 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, 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. Our support to TSA to develop a recent Security Directive requiring reporting of cybersecurity incidents to CISA is an important step and an example of such collaboration. We look forward to working with Congress to further encourage reporting of cybersecurity incidents to CISA in order to further enable this essential visibility.

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.

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 are segmented from, and can run independently of 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 malicious cyber activities 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.