TESTIMONY OF

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

BEFORE

Select Committee on Strategic Competition Between the United States
and the Chinese Communist Party
United States House of Representatives

ON

The CCP Cyber Threat to the American Homeland and National Security

January 31, 2024
Washington, D.C.

Chairman Gallagher, Ranking Member Krishnamoorthi, and Members of the Committee, thank you for the opportunity to testify regarding the Cybersecurity and Infrastructure Security Agency's (CISA) efforts to respond to cyber threats to the United States from the People's Republic of China (PRC).

As America's cyber defense agency, CISA has long been concerned about the breadth, depth, and sophistication of the PRC cyber threat to the United States. Our cyber operations protect critical infrastructure by ensuring U.S. businesses and government agencies receive actionable information, guidance, and technical assistance to defend against those risks.

Over the last two years, we have become increasingly concerned about a strategic shift in PRC malicious cyber activity against U.S. critical infrastructure. As the Director of National Intelligence highlighted last year,[1] the PRC is accelerating the development of military capabilities—including cyber operations—it believes are needed to deter and confront the United States. We are deeply concerned that PRC actors—particularly a group referred to in industry reporting as Volt Typhoon—are seeking to compromise U.S. critical infrastructure to pre-position for disruptive or destructive cyber attacks against that infrastructure in the event of a conflict to prevent the United States from projecting power into Asia or to cause societal chaos inside the United States. Our intelligence community has noted that some of the entities impacted by this activity are not targeted for their intelligence value, but are instead targeted for potential disruptive or destructive attacks.

Working with our government and industry partners, we are assisting several critical infrastructure entities across multiple sectors that already have been compromised by Volt Typhoon actors. In many cases, the PRC actors are maintaining presence on victim organization networks by using advanced techniques that make finding and remediating such intrusions more challenging than with more commonly used tactics. Based on our insights from working with victims of these intrusions and industry partners with unique visibility into these threats, PRC cyber actors are almost certainly capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems.

For CISA, these developments spur us to collaborate with our partners across government and industry to proactively reduce risks in the face of the most pressing threats. We are pursuing three tracks of engagement to reduce risks to the American people. First, we are helping victims identify and evict PRC actors from their networks. Second, we are working with industry partners to identify and drive effective mitigation approaches across targeted sectors and technology products. Third, we are taking steps to drive broader resilience investments to reduce the likelihood that a cyber intrusion could result in functional impacts to the services Americans rely on every day.

Victim Engagement and Support

Every day, CISA works with government partners such as the Federal Bureau of Investigation (FBI) and sector risk management agencies (SRMAs) to identify and notify victims of cyber intrusions. Presently, we are engaged with multiple U.S. critical infrastructure owners and operators to hunt for PRC actors and help remediate any intrusions. We use findings from

[1] Office of the Director of National Intelligence, "2023 Annual Threat Assessment of the U.S. Intelligence Community," March 8, 2023, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/3676-2023-annual-threat-assessment-of-the-u-s-intelligence-community.

these activities to inform detection and mitigation guidance that CISA and its partners provide to federal entities, state, local, tribal, and territorial (SLTT) partners, private sector entities, and international allies. These efforts build off the cybersecurity advisory "PRC Cyber Actor Living off the Land to Evade Detection"[2] that was jointly published last year by CISA, the National Security Agency (NSA), and FBI, along with our international cybersecurity partners from Australia, Canada, New Zealand, and the United Kingdom (UK), to help organizations hunt for and remove this PRC activity on their systems. Our goal is to create a virtuous cycle in which our identification of PRC cyber activities enables refinement of our detection guidance and capabilities, which will enable broader identification and remediation. We are additionally deploying numerous capabilities to help detect and reduce the likelihood of PRC intrusions, including:

- Our **CyberSentry** platform, a threat detection and monitoring capability for information technology and operational technology, provides us with persistent visibility into adversary activity targeting select critical infrastructure networks and the ability to support urgent mitigation where activity is identified. We now have nearly 30 entities participating in CyberSentry, including major pipelines, energy generation facilities, a large airport, and critical manufacturing facilities, with about 15 more entities expected to participate by the end of this year.
- Our **Attack Surface Management** services are used by nearly 7,000 organizations to identify weaknesses in Internet-facing systems and allow CISA to pinpoint organizations with specific vulnerabilities known to be used by PRC actors, including those in our **Known Exploited Vulnerabilities** catalog, to drive targeted mitigation before intrusions occur.
- Our **Critical Infrastructure Shared Services** pilot, first funded by Congress last year, provides scalable best-in-class protection capabilities to "target rich, resource poor" organizations such as water utilities and hospitals to prevent threat actors from launching attacks or stealing data through malicious web domains.

Industry Engagement

As a government, we cannot tackle this threat alone. We must maintain robust operational collaboration with the private sector—which is why the Joint Cyber Defense Collaborative (JCDC), and the groundwork laid since its establishment in August of 2021, has been so critical to our success. The private sector often has unique insights into the scope and scale of PRC cyber threats, including from Volt Typhoon. It is only through focused operational collaboration with the private sector that we can fully understand the depth and breadth of PRC cyber threats to the Nation. CISA then provides tailored guidance to assist critical infrastructure owners and operators to detect and mitigate PRC cyber threats. Our industry engagement includes working alongside SRMAs to provide over 70 briefings across the 16 critical infrastructure sectors since last summer, which included threat overviews and specific guidance on how to defend against PRC cyber threats.

Another pillar of CISA's cybersecurity work is our cybersecurity defense planning. CISA engages in joint planning with a range of critical infrastructure partners to create common, shoulder-to-shoulder approaches to confront malicious actors and significant cyber risks. CISA,

[2] Joint Cybersecurity Advisory, "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection," May 24, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.

through the JCDC, has initiated a cyber defense planning effort focused on the defense of U.S. critical infrastructure networks from Volt Typhoon-related malicious cyber activity. We are working with our public and private sector partners to understand Volt Typhoon's targeting of U.S. critical infrastructure and to take coordinated defensive measures to mitigate this activity.

Driving Long-Term Security and Resilience

As we work to detect PRC cyber activities, our cybersecurity advisors across the country work with critical infrastructure organizations every day to conduct Cybersecurity Performance Goals assessments driving investments in the most impactful security measures to prevent, detect, and respond to advanced threats like Volt Typhoon. While these efforts are necessary, we know that sustained improvements also require more secure technologies. Sophisticated cyber actors like Volt Typhoon frequently use defects in technology products to compromise victims and gain a persistent presence on target networks. These weaknesses can be mitigated by manufacturers delivering products that are secure by design.

Strong security should be a standard feature of every technology product, especially those that support U.S. critical infrastructure. Technology must be purposefully developed, built, and tested to reduce the number of exploitable flaws before it is introduced into the market for broad use. Achieving this outcome will require a significant shift in how technology is produced, including the code used to develop software. Such a transition to Secure by Design products will help both organizations and technology providers. It will mean less time fixing problems and more time focusing on innovation and growth, and, importantly, it will make life much harder for our adversaries. Together, we must break the cycle of finding security defects after customers have deployed products and then requiring those customers to fix those defects at their own expense.

Further, we launched our Shields Ready campaign to drive key resilience measures. This campaign is designed to help all critical infrastructure stakeholders take actions to enhance security and resilience by providing recommendations, products, and resources. We know that no defense will be 100 percent effective, so we must have the ability to be resilient in the face of an incident and recover from disruptions of critical services.

Closing

The PRC's malicious cyber activity—including its preparations for cyber attacks against U.S. critical infrastructure—poses a serious threat to the United States and our partners worldwide that requires a coordinated response to drive comprehensive risk reduction. In our role as America's cyber defense agency and the national coordinator for critical infrastructure security and resilience, CISA, in collaboration with our government partners, will continue to drive efforts focused on countering this challenge.

I am proud of the work that CISA and our partners in government and industry have undertaken in response to PRC cyber threats. I also recognize that we have more to do to defend our critical infrastructure from a broad array of threats. CISA is committed to addressing these threats. I look forward to working with Congress to ensure CISA has the authorities and resources necessary to defend the American people.

Thank you for the opportunity to appear before you today, and I look forward to your questions.