**Testimony of Dr. Charles Clancy**

**Chief Technology Officer, MITRE**

**before the House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection, Hearing on Securing Operational Technology: A Deep Dive into the Water Sector**

*6 February 2024*

Chairman Garbarino, Ranking Member Swalwell, and Committee Members:

Thank you for inviting me to testify before you today on a topic of critical national importance. My name is Charles Clancy, and I am a Senior Vice President and Chief Technology Officer at MITRE where I lead science, technology, and engineering for the company. MITRE is a non-profit, non-partisan research institution that operates Federally Funded Research and Development Centers (FFRDCs) on behalf of the U.S. Government. Among other technical disciplines, our team of over 1,500 cybersecurity professionals provide deep expertise across the executive branch, including in support of organizations like the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and U.S. Cyber Command. MITRE's ATT&CK™ framework has become the *de facto* language between government and industry for describing and combatting cyber threats.

Prior to joining MITRE, I spent nine years as a member of the faculty at Virginia Tech where I held the Bradley Distinguished Professorship of Cybersecurity in the Department of Electrical and Computer Engineering, and served as executive director of what is now the Virginia Tech National Security Institute. I started my career at the National Security Agency leading advanced research and development programs.

It is my pleasure to address this committee.

***Threat Environment***

Threats to our nation's critical infrastructure cybersecurity have heightened dramatically over the past seven years as Russia and China have shifted to using cyber access to U.S. critical infrastructure as a strategic instrument of statecraft. Targeting and penetrating our infrastructure have grown precipitously, leading then Director of National Intelligence Dan Coats to famously say the "warning lights are blinking red again" in 2018[1], comparing warning signs about critical infrastructure penetrations to the pre-9/11 indicators. Just last week FBI Director Christopher Wray testified that the U.S. government had successfully disrupted Volt Typhoon[2], a persistent and sophisticated Chinese Communist Party (CCP) campaign to gain strategic access to U.S. critical infrastructure systems for disruptive and destructive effects.

In its 2023 annual threat assessment[3], the intelligence community assessed that the CCP would launch widespread cyber attacks against US critical infrastructure ahead of an invasion of Taiwan to "deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces." Their primary targets are assessed to be energy, transportation, communications, and water infrastructure.

With President Xi's asserted timeline of being ready for a Taiwan invasion by 2027[4], the U.S. military is kicking its response planning into high gear, but the U.S. may be existentially unprepared to defend its critical infrastructure for what would undoubtedly be an initial wave of attacks, followed by a sustained cyber campaign targeting U.S. infrastructure. Campaigns like Volt Typhoon demonstrate that this threat is not hypothetical: the CCP is deliberately gaining access to critical infrastructure so it can strategically disrupt and destroy these systems at a future time.

Much of the U.S. strategy to date has focused on strengthening our systems to keep adversaries out of our critical infrastructure and to blunt the first wave; however, this strategy fails to recognize that CCP attacks in conjunction with a Taiwan invasion will not be discrete events for which we can respond proportionately, but an enduring cyber conflict. Our current

---

[1] https://www.npr.org/2018/07/18/630164914/transcript-dan-coats-warns-of-continuing-russian-cyberattacks
[2] https://www.washingtonpost.com/national-security/2024/01/31/china-volt-typhoon-hack-fbi/
[3] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf
[4] https://www.reuters.com/world/china/logistics-war-how-washington-is-preparing-chinese-invasion-taiwan-2024-01-31/

approach is inadequate. Advanced persistent threat actors are frequently obviating protections we have placed in these systems. It also doesn't address the rapid response and restoration activities that will inevitably be needed to reconstitute when attacks occur.

***Needed Strategic Posture***

Much can be done to improve the current apparatus for securing critical infrastructure, and I will address those within the context of the water sector shortly. But I fear those actions miss the forest for the trees.

Nationally, we need to prepare for a more realistic adversary operational plan. Military systems have *wartime reserve modes* that change their configuration and operating posture to confound adversary exploitation, and the U.S.'s critical infrastructure systems need an intellectually similar set of contingencies that can be activated in a period of major conflict.

Many critical infrastructure operators already contemplate such impacts through the lens of natural disasters. For example, electric grid operators consider ways to minimize the impacts of geomagnetic disturbances from the sun by modifying the state and configuration of their operations. This operational adaptability mindset needs to extend to cyber-attack scenarios.

Operators need to prepare, train, and exercise for isolation operations where they operate their operational technology (OT) systems physically isolated from the information technology (IT) systems and the Internet. This includes creating continuity of operations plans that sever IT and OT systems to disrupt an adversary's ability to command and control malicious tools deployed into OT systems. Given CCP threat actors have adopted a strategy of "living off the land" where they do not install detectable malicious agents in target networks, but rather access systems like authorized administrators[5], severing IT-OT connectivity would prevent them from triggering effects to degrade or destroy critical infrastructure sytems.

Likely many critical infrastructure operators lack the needed engineering staff to sustain isolation operations in an ongoing capacity, so new programs are needed to train national guard units or create a civilian reserve corps of cyber physical operators and experts to augment critical infrastructure operators to sustain isolation operations. Moreover, we need to practice for multiple sector failures in population centers and assess cascading impacts. This includes not

[5] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

only tabletop exercises and hypothetical wargaming, but also live drills where we test contingency operations.

The cost of compliance is a common pushback to levying new responsibilities on private sector critical infrastructure asset-owner-operators, therefore, to incentivize adoption of cyber best practices, the federal government needs to reduce that burden. The Federal Emergency Management Agency (FEMA) should extend their existing grants program[6], in partnership with Sector Risk Management Agencies (SRMAs), to fund the necessary preparation, training, and exercises. The Cybersecurity Infrastructure Security Agency (CISA) should be resourced to manage a systematic exercise program to ensure that, if necessary, we have the national experience necessary to act under urgent circumstances.

Given the scale of the challenge, FEMA and CISA should focus on the current CISA *lifeline* sectors: energy, water, communications, and transportation[7].

***Water Sector***

The water sector is perhaps the most under resourced and disadvantaged among the lifeline sectors. In addition to preparing and practicing contingencies for a large-scale and enduring cyber conflict, there are plenty of more targeted things that could help improve cybersecurity and make China and Russia's cyber exploitation efforts more difficult.

Presidential Policy Directive (PPD) 21[8], *Critical Infrastructure Security and Resilience*, and PPD 41[9], *United States Cyber Incident Coordination,* organized the ecosystem we have today between CISA, the Federal Bureau of Investigation (FBI), and SRMAs. Accordingly, SRMAs bear the front-end regulatory responsibilities, while CISA and the FBI are responsible for back-end incident management and investigation after a cyber attack has occurred. There is a perception by operators, however, that systematically engaging SRMAs in incident response could lead to punitive regulatory actions. That, combined with their frequent lack of incident response experience and expertise, leads to an open loop system where we do not learn from

---

[6] https://www.cisa.gov/state-and-local-cybersecurity-grant-program
[7] https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf
[8] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[9] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

attacks, which is antithetical to the goals of the NIST Cybersecurity Framework[10] and Executive Order 13636[11]. While sectors like the bulk electric power system[12] have been forced to ameliorate this through robust working-level relationships, public-private partnerships, and unique authorities held by the Secretary of Energy[13], other sectors such as water lack this scale, sophistication, and authorities.

At a national level, water's SRMA, the Environmental Protection Agency (EPA) needs to deepen its in-house cybersecurity expertise and develop a strategy to promote cybersecurity more effectively within the sector. This strategy should be informed by threat and incident information by EPA being much more engaged with CISA in incident response and analysis. The recently released incident response guide[14] is a good indicator that these connections are strengthening. Given the large number of water entities without any cybersecurity expertise and limited resources, implementation guidance, in plain language, will likely be needed to translate existing CISA, FBI, and NSA guidance to a simplified list of priority actions.

Grass-roots efforts being led by the Water Sector Coordinating Council and Water Information Sharing and Analysis Center (ISAC) are also important positive steps. In fact, both MITRE and Dragos are working closely with the Water ISAC on constructive solutions[15]. More broadly, MITRE has recommended SRMAs shift the focus from compliance checking to self-assessments, threat sharing, technical assistance, and fostering the organizational capacity and expertise execute[16].

Another important step is standardizing reporting of cyber incidents. Despite highlighting significant cybersecurity gaps within the water sector, prior EPA efforts were

---

[10] https://www.nist.gov/cyberframework
[11] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[12] https://www.nerc.com/pa/Stand/Pages/default.aspx
[13] https://www.energy.gov/ceser/energy-security-provision-within-fixing-americas-surface-transportation-act-fast-act
[14] https://www.cisa.gov/resources-tools/resources/water-and-wastewater-sector-incident-response-guide-0
[15] https://www.waterisac.org/portal/water-and-wastewater-utilities-and-other-critical-infrastructure-fortify-defenses-against
[16] https://www.mitre.org/sites/default/files/2023-11/PR-23-02057-08-Cybersecurity-Regulatory-Harmonization.pdf

withdrawn over legal challenges[17]. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022[18] offers the potential to close this gap if the information collected is robust and focused on reporting tangible threat behaviors and indicators. Similarly, improved coordination and interoperability among OT security vendors[19] could also help close the information and reporting gap.

Meanwhile, since Executive Order 14028[20], industrial capacity to generate and deliver software bills of material (SBOMs) has been improving. Open-source software underpins most of the Internet, and is also pervasive in OT networks. In most cases, this software has dubious supply chains[21] and critical infrastructure operators need tools to better manage this risk. One approach is to have OT vendors selling into the U.S. market provide SBOMs for their products to a clearinghouse that notifies them if a new vulnerability is disclosed that impacts their product. Much like safety recalls for automobiles governed by the National Highway Traffic Safety Administration (NHTSA), similar notices could be combined with regulatory rulemaking to prompt critical infrastructure operators to close security gaps in a timelier manner.

***Conclusion***

In closing, there is a considerable opportunity for EPA to step up, CISA and FBI to systematically engage across, and the network of security vendors to make it easier for everyone to coordinate. But these modest reforms should be kept in context with the scale of the threat, and the limited amount of resources available to critical infrastructure operators, particularly in the water sector. We should urgently begin piloting, exercising, and preparing for contingency scenarios that require isolated operations across lifeline critical infrastructure sectors.

---

[17] https://www.securityweek.com/epa-withdraws-water-sector-cybersecurity-rules-due-to-lawsuits/

[18] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

[19] https://www.nozominetworks.com/blog/ethos-emerging-threat-open-sharing-platform

[20] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[21] https://industrialcyber.co/reports/fortress-research-finds-most-us-energy-software-contains-code-from-russian-chinese-developers/