Dr. Nate Gleason

Program Leader, Cyber and Infrastructure Resilience Program, Lawrence Livermore National Laboratory

Testimony before the Subcommittee on Cybersecurity and Infrastructure Protection of the Committee on Homeland Security

July 22, 2025

Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson and Members of the Subcommittee, thank you for the opportunity to testify today.

My name is Dr. Nate Gleason, and I am the Program Leader for the Cyber and Infrastructure Resilience Program at Lawrence Livermore National Laboratory (LLNL) in Livermore, California. I am honored to be here today on behalf of LLNL, a National Nuclear Security Administration (NNSA) laboratory and proud member of the Department of Energy's network of national laboratories.

At the Lab, I have the privilege of leading a multidisciplinary team that includes operational technology (OT) cyber experts, threat hunters, reverse engineers, data scientists, electrical/chemical/civil/mechanical engineers, computer scientists, systems analysts and intelligence analysts in a program focused on providing the U.S. with technologies to effectively compete with nation-state adversaries like Russia and China in the domain of gray-zone conflict. Our primary emphasis is on the role of critical infrastructure in national security. I sincerely appreciate the Committee's interest in the work we do in support of the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy (DOE), the Department of Defense (DOD), and U.S. critical infrastructure writ large, as evidenced by your visit to the lab earlier this summer.

Nearly everything we do as a nation, whether it be critical national functions like energy transmission or our ability to defend our homeland and project force around the globe, depends on critical infrastructure. As reflected in reports on Volt Typhoon and other threat actors, our adversaries see our critical infrastructure as an attractive target. As CISA and the Intelligence Community (IC) have acknowledged, these adversaries seek to pre-

position themselves on U.S. critical infrastructure networks for disruptive or destructive cyber attacks. These adversaries are highly capable and invest significant resources in developing capabilities to hold our infrastructure systems, and the functions that depend on them, at risk. To defend against this threat, the U.S. must out-innovate the competition, work across federal, state and local authorities, and link with the public and private sectors to bring our best technology into operations.

CyberSentry

CISA plays a key role in bolstering critical infrastructure cybersecurity. The CyberSentry program is an excellent example of how CISA leverages government capabilities to identify and mitigate highly consequential cyber threats targeting critical infrastructure, and I would like to thank the Committee for its leadership on this program.

Through CyberSentry, CISA works with private sector partners who volunteer to have their systems monitored for malicious activity. Participants are from a wide range of critical infrastructure sectors including energy; water and wastewater; transportation; chemical; nuclear reactors, materials and waste; food and agriculture; dams; and critical manufacturing. Since 2020, LLNL has provided core support to the program by developing advanced analytic capabilities and leveraging artificial intelligence (AI) to detect novel adversary techniques and then deploying those analytics to operationally monitor and hunt for threats in the partner networks.

CyberSentry is valuable because it provides cyber researchers real-time access to real-world systems and network data so that we can take information on adversary intent, capability and activity from the IC, combine it with the technological and computational resources of the DOE national laboratories, and develop and deploy new tools to detect and mitigate the latest techniques of our adversaries. CISA uses the data generated from our work to then create alerts for the broader U.S. critical infrastructure operator and owner community.

2022 Discovery of Chinese Surveillance Cameras on U.S. Critical Infrastructure Networks

One of LLNL's most notable contributions to the CyberSentry program was when, in 2022, we detected high-risk Chinese surveillance cameras that were stealthily built into U.S. critical infrastructure systems. CISA had asked LLNL to develop a capability to detect subtle malicious beaconing behavior that available tools could not detect. Using our

hardware-in-the-loop laboratory (dubbed the “Skyfall” lab), LLNL set up an operational technology (OT) environment where we deployed various samples of beaconing malware and tested existing commercial and open-source tools. We then developed a more advanced beacon detection analytic that built on the performance of the existing tools, both increasing the sensitivity so that it could detect more subtle threats and improving the selectivity to dramatically reduce false positives, and deployed it in the CyberSentry environment.

Almost immediately after deploying the new analytic, our threat analysts detected anomalous beacons on the OT network of a participating company. Working with that critical infrastructure partner, we identified the beaconing device as a security camera manufactured by the Chinese company Dahua, which is listed on the Federal Communications Commission (FCC) Covered List.

With this detection, we were able to create a machine learning model to automate detection of these cameras and deploy it widely across participating CyberSentry partners. Working with CISA, we discovered that the majority of entities in the program had these cameras on their networks. In some cases, we found hundreds of these devices on individual networks.

Notably, not all of the devices detected were branded as Dahua devices; many other manufacturers, both foreign and domestic, sold devices that used the same components as the Dahua camera and were behaving identically. From the network traffic, we were able to observe the devices beaconing back to suspected hostile overseas servers. Some of the devices were observed sending what appeared to be encrypted video to those servers. After acquiring and analyzing some of these devices, our reverse engineers were able to identify additional functionality that could enable back-door access to any network to which the device was connected. For purposes of today’s discussion, it is worth noting that many of these cameras were sitting on OT networks, potentially granting access to control the physical processes in our infrastructure.

CISA partnered with the Department of Energy’s Office of Cybersecurity, Energy Security and Emergency Response (CESER) and the DOE Office of Intelligence and Counterintelligence (DOE IN) to communicate our findings, first throughout the IC and then broadly out to the energy sector. Among the products of this collaboration was a set of playbooks we created that were published by CISA that allowed asset owners to detect these devices in their own systems. In this way, the security gains derived from this partnership between a few dozen critical infrastructure asset owners and CISA reverberated widely across U.S. critical infrastructure.

Immune Infrastructure Framework

Detection and mitigation represent just one aspect of defense against nation-state cyber threats to our critical infrastructure. Today, we are dealing with highly capable adversaries who bring a wide spectrum of capabilities to bear, including network operations, supply chain compromise, insider access, and close-access operations. The current threat picture demands that we take a multi-layer approach to ensure the resilience of the functions that depend on our infrastructure.

At LLNL, we approach the challenge of securing U.S. critical infrastructure through a structure called the "Immune Infrastructure Framework." We developed this framework to help define the parameters of critical infrastructure resilience and identify strengths and gaps in our nation's capabilities. It is largely reflected in the approach taken within DOE to help protect the energy sector, including the DOE Cyber Resilience R&D Capabilities Catalog issued by the DOE Chief Information Officer (CIO). The Immune Infrastructure Framework accepts that it is not practical to prevent all compromises, and structures defense in four layers to make it as difficult as possible for adversaries to achieve their goals and enable our critical infrastructure to operate through compromise.

- Layer 1 focuses on understanding U.S. critical infrastructure systems. This involves developing tools to characterize, model, and analyze our critical infrastructure so that we can understand our vulnerabilities and also identify where the most attractive targets for an adversary might be. This essentially allows us to look at U.S. infrastructure through the eyes of our adversaries.

- Layer 2 attempts to keep the adversary out of our systems. This largely involves assuring our supply chain to minimize both vulnerabilities and malicious functionality on the devices and software we put into our infrastructure systems. A key emphasis is on creating scalable capabilities to allow us to exponentially increase the number of devices that can be examined that are present within U.S. critical infrastructure.

- Layer 3 focuses on detecting and responding to intrusions in our systems. The majority of cyber attacks on critical infrastructure come from lower tier adversaries – individual hackers, criminal organizations, hacktivist groups – and use known malware and established tactics. The commercial security industry is quite capable of detecting these threat signatures and known adversary behaviors, so as a national laboratory we focus on "zero day" threats. We use advanced analytics and AI in conjunction with information from the IC to detect novel adversary tactics,

capabilities, and activities that do not necessarily involve malware. More specifically, as a national security lab, we put significant energy towards assessing the unique capabilities that China, Russia, and Iran are developing that could hold our systems at risk that may never have been seen before.

- Layer 4 is about engineering our systems to operate through compromise. Despite our best efforts, the most determined and capable adversaries will compromise our systems; we must build in resilience by leveraging the distributed nature of our infrastructure and using techniques like collaborative autonomy, a set of algorithms designed to provide redundant, decentralized control of the system.

Support for Sector Risk Management Agencies

As defined in Presidential Policy Directive 21, CISA coordinates the national effort to secure and protect against critical infrastructure risks, but securing our nation's critical infrastructure is a distributed responsibility. There are 16 critical infrastructure sectors, with responsibilities distributed across Federal agencies, State and local governments, and asset owners and operators.

While all of the sectors are important, at LLNL, we pay particular attention to four sectors because of their close connection to national security concerns – energy, water, transportation, and communications. Sector Risk Management Agencies, such as DOE and DOD, have significant responsibilities to provide sector-specific expertise and coordinate activities within their sectors. We and our partners at other DOE national laboratories serve a vital connective tissue between Sector Risk Management Agencies, States, and local utilities and work directly with private sector entities to help ensure efforts are coordinated.

Among the sectors, the energy sector tends to be one of the most forward-leaning about cybersecurity because of the interdependencies between energy and every other sector. For its part, DOE CESER invests resources in creating capabilities for the energy sector that, in coordination with CISA, help set the pace for other sectors. For example, DOE is leaning forward to support industry in integrating AI securely. LLNL is leading CESER's analysis of the potential risks and benefits of AI to the energy sector. We are also developing testbeds for CESER to assess both the security and efficacy of various AI capabilities for the energy sector and researching new AI capabilities to improve the security and resilience of U.S. energy infrastructure.

Another way CESER is working to enhance the cybersecurity of the energy sector is through its Energy Cyber Sense Program which illuminates and reduces vulnerabilities to supply chains. LLNL leads national security-focused efforts as part of this work. LLNL also develops advanced tools and methodologies to understand and automate supply chain assurance with some of the critical partners in industry involved in these efforts.

In addition to our work on behalf of CISA and CESER efforts, our program has worked closely with the DOD, DOE, and CISA on efforts to enhance the security and resilience of Defense Critical Infrastructure (DCI). These assets are those portions of our nation's infrastructure that directly contribute to the mobilization and sustainment of military forces. We lead DOE's Defense Critical Energy Infrastructure analysis efforts and support multiple offices in DOD for broader DCI efforts. Our work has been critical in identifying potential risks posed by adversaries who, with advanced knowledge of our infrastructure and the interdependencies that exist between different components, could target assets in combination to cause damage that could not be realized in a single attack against one asset. LLNL's high-performance computing modeling and simulation capabilities and advanced optimization tools, codified in the Octopus and Teragrine toolsets, move beyond traditional natural hazard-focused planning processes which often only consider failures of single system elements and are not designed to identify cascading consequences from multiple simultaneous disruptions.

Conclusion

Thank you again for giving me the opportunity to share with you how LLNL, as a DOE national laboratory, deploys its multidisciplinary teams in partnership with CISA, CESER, DOD and other Federal partners to bolster the cybersecurity of the nation's critical infrastructure systems and advance U.S. national security. I would be happy to answer any questions.