Congress of the United States

Washington, DC 20515

July 14, 2026

The Honorable Nick Andersen
Acting Director
Cybersecurity and Infrastructure Security Agency
245 Murray Lane SW
Washington, DC 20528

Dear Acting Director Andersen,

We write today as Chairman and Ranking Member of the National Intelligence Enterprise Subcommittee of the House Permanent Select Committee on Intelligence to express our great concern over cyber vulnerabilities in U.S. manufacturing and critical infrastructure following recent reports of a Russian cyberattack—potentially state-backed— of Jaguar Land Rover (JLR) in the United Kingdom (UK) in August 2025. The sabotage operation last year reportedly suspended JLR production for five weeks and cost the UK economy $2.5 billion, making it the largest cyberattack in the UK's history.[1] Given that JLR is a major component of the UK defense industrial base, the attack raises significant concerns over Russian-backed efforts to sabotage manufacturers critical to defense supply chains here in the United States as well. Therefore, we urge you to develop and share a strategy to thwart such attacks and outline how you will support stronger cyber defenses across American companies, government networks, and critical infrastructure.

Last week, the *New York Times* reported that a group of Russian hackers were behind the Jaguar hack.[2] The cyberattack— which reportedly included a "mind-blowing" ransomware encryption algorithm— forced Jaguar to shut down its computers and halt production in five countries across three continents,[3] negatively impacting tens of thousands of jobs and smaller parts manufacturers that form the backbone of major industrial supply chains. While authorities are still determining the extent of the involvement of the Russian state, this cyberattack must cause us to question our own cyber defenses and whether cyber actors could infiltrate U.S. systems to shut down defense production and/or disrupt access to critical infrastructure including communications, electricity, transportation, and water.[4]

In addition, the JLR hack is a further escalation of likely Russian state-backed cyber-attacks that pose a threat to NATO members' critical infrastructure and supply chain security. As the battlefield turns against Russian forces in Ukraine, Putin's regime is increasingly turning to other means to weaken the United States and its allies. This kind of grey-zone activity shows Russia's growing willingness and ability to deal major blows to adversary infrastructure and economies while ensuring it stays below the threshold of a major geopolitical response.[5] While the FBI has worked to support British intelligence and investigations into the Jaguar cyberattack, the FBI and other members of the Intelligence Community also need to work in coordination with American companies, as well as utilities, to ensure that foreign actors do not gain access to the systems required to ensure our national security, and if they have access, to ensure those vulnerabilities are patched.

---

[1] Goldman, Adam, Jane Bradley, Dustin Volz, and Michael Schwirtz. "A $2.5 Billion Whodunit: The Hack That Dented the U.K. Economy." The New York Times, June 26, 2026.
[2] *Id.*
[3] *Id.*
[4] Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure § (2025). https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a.
[5] Morley-Davies, Joe. Deterring Kremlin Grey Zone Aggression Against NATO, August 29, 2025. https://www.rusi.org/about/our-heritage/rusi-history.

To that end, please provide responses to the following questions by July 28, 2026:

1. What assessment has CISA made of the cybersecurity posture of the U.S. defense industrial base with respect to disruptive ransomware and cyberattacks designed to halt production rather than just steal data?
2. Has CISA identified any sectors of U.S. critical infrastructure or manufacturing that are particularly vulnerable to a Jaguar-style attack? If so, what steps are being taken to address those vulnerabilities?
3. Is there currently any evidence of similar network infiltrations, state-backed or otherwise, in the United States?
4. What lessons, if any, has CISA drawn from the Jaguar incident, and how are those lessons being incorporated into guidance, assessments, or cybersecurity programs for U.S. industry?
5. What is the Department of Homeland Security (DHS) and CISA's current capacity to share threat indicators from foreign incidents like Jaguar with U.S. private sector partners in real time? How have the resource and personnel cuts since January 1, 2025 impacted CISA's capacity to share information with the private sector?
6. What additional actions are DHS and CISA taking to protect American companies and critical infrastructure from these kinds of hacks? Does DHS have a government-wide strategy to thwart these kinds of hacks?
7. How has the administration pushed back against nation-state sabotage efforts in the United States or among our treaty allies?
8. How is CISA working to ensure that small and medium-sized manufacturers—many of which lack dedicated cybersecurity personnel—receive timely threat intelligence and cybersecurity assistance? Does CISA have the proper resources to support this effort?
9. What authorities does CISA currently lack, if any, that would improve its ability to identify or mitigate threats to critical infrastructure and manufacturing networks?

We look forward to your timely response.

CC: Kash Patel, Director, FBI

Sincerely,

Raja Krishnamoorthi
Member of Congress

Austin Scott
Member of Congress