Congress of the United States

Washington, DC 20515

November 17, 2026

The Honorable Walter "Jay" Clayton III
Director
Office of the Director of National Intelligence
1500 Tysons McLean Drive
McLean, VA 22102

Dear Director Clayton:

We write to urge the Super Intelligence Task Force to launch a national effort to confront a new generation of AI-enabled cyber threats. AI is rapidly increasing the ability to discover and exploit weaknesses in software, and our defenses are not keeping pace.

Four recent developments underscore the urgency:

- First, last month, AI uncovered decades-old serious vulnerabilities in PHP, software used by millions of websites, leading to governments and companies shutting down their websites to patch the flaws. CNN reported that this vulnerability could affect up to 70% of websites globally.
- Second, major U.S. banks have reported they are confronting unauthorized AI agents that have accessed customer accounts. In some instances, banks cannot tell whether the AI agent has been deployed on behalf of the customer or is a rogue actor. Banks are concerned that agents could access sensitive financial information or initiate transactions without proper authorization, and are strengthening security protocols to identify and control such activity.
- Third, in Japan, a recent spate of cyberattacks against companies and financial institutions led to large-scale data breaches and leaks, which the Japanese government is now seeking to contain. These developments illustrate the growing exposure of our digital infrastructure to sophisticated cybersecurity threats bolstered by the power of AI.
- A fourth concern is emerging with foreign-developed AI models. In a recent security test, researchers at Cohere reported that a Chinese-developed Qwen model attempted an unauthorized connection to a server in China. Although the finding does not establish deliberate malicious behavior, it underscores the risk that AI models could introduce vulnerabilities, make unauthorized connections, or compromise sensitive systems without users' knowledge.

The fundamental problem is that AI can discover software weaknesses and help attackers exploit them faster than many organizations can respond. Even when fixes are available, testing and installing patches across interconnected systems can take weeks or months, potentially disrupting

essential services. At the same time, autonomous AI agents capable of writing code, accessing sensitive systems, and taking actions independently are introducing new security risks. We cannot meet these threats with yesterday's cybersecurity infrastructure or rely on individual companies to solve a problem that spans the entire digital economy.

We therefore urge the Super Intelligence Task Force to convene leading AI developers including open-source developers, cybersecurity companies, critical infrastructure operators, the National Institute of Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA), other appropriate federal agencies, and the National Laboratories around two urgent defensive priorities:

1. **Use the full suite of cyber tools to secure our existing digital infrastructure**. This includes using defensive AI-powered tools that continuously identify vulnerabilities, develop and test fixes, and detect and block attacks before they spread. But finding vulnerabilities is not enough. Organizations also need ways to protect exposed systems immediately, including patching to block attacks and installing permanent fixes. NIST, working with relevant federal agencies, industry, academic researchers, and independent security experts, should develop risk-based guidance, evaluation methods, and standards for defensive AI tools.

CISA should help accelerate their adoption across critical infrastructure. To protect our U.S. economy and the public, these capabilities must reach banks, hospitals, utilities, small businesses, and government agencies—not just the largest technology companies. Priority should also be given to securing federal websites, widely used software that underpins the internet, and the supply chains supporting national security, including defense contractors. This effort should build on existing open cybersecurity standards and industry initiatives, including the Linux Foundation's Open Secure AI Alliance.

2. **Secure the AI agents we use to discover vulnerabilities in systems**. The same agents that can discover vulnerabilities and repair software can also introduce dangerous code, exceed their instructions, or gain unauthorized access to sensitive systems. These risks include agents that introduce vulnerabilities into software, conceal unauthorized activity, or make connections to external systems without authorization. NIST should lead the development of security standards for defensive AI agents and the environments in which they operate, including standards for secure testing environments, limits on system access and permissions, and continuous monitoring. These standards should also address the security of the models and software supply chains on which agents depend, including risks associated with foreign-developed models. These standards should strive to make AI agent behavior explainable, independently verifiable through testing, and subject to audits that assess whether organizations maintain effective security controls.

These two priorities must advance together. More powerful defensive AI will accomplish little if organizations cannot use it quickly and safely. And expanding autonomous AI without effective security controls risks creating new vulnerabilities even as we close existing ones.

To translate these priorities into action, we urge the Task Force to launch a national cyber defense grand challenge. Building on proposals such as the Institute for Progress's Operation Patchlight, the initiative should mobilize government, industry, National Laboratories, and researchers to use AI to find and fix vulnerabilities in widely used software and critical parts of the web. The challenge should demonstrate, across participating federal systems, critical infrastructure, and defense supply chains, that AI-enabled defenses can cut the time from discovery of a critical vulnerability to effective protection. NIST should establish independent methods to measure performance and security, including the speed and reliability of fixes and relevant agencies should coordinate practical deployment and help scale successful approaches nationally.

The United States has the technological expertise to lead this effort. What is missing is a coordinated national strategy to bring these capabilities together, establish common security standards, and put effective defenses into widespread use.

We urge the Super Intelligence Task Force to make these priorities central to its mission and develop a concrete plan for federal agencies and industry to act. That plan should identify a national grand challenge, assign agency responsibilities, establish measurable milestones, and specify the resources and authorities needed to carry it out. AI is changing cybersecurity at unprecedented speed. Our national response must match that urgency.

Sincerely,



Maria Cantwell
United States Senator

Ranking Member
Committee on Commerce, Science and Transportation



M. Michael Rounds
United States Senator

Chair
Subcommittee on Cybersecurity, Senate Committee on Armed Services

Co-Chair
Senate Artificial Intelligence Caucus