Stay Current

PAUL HASTINGS

July 2026

Follow us on LinkedIn

PH Privacy

White House Launches ‘Gold Eagle’ AI-Driven Cybersecurity Vulnerability Clearinghouse

By Aaron Charfoos, Michelle Reed, Amir Ghavi and Jeremy Berkowitz

On July 14, the White House announced the launch of “Gold Eagle,” a new federal clearinghouse designed to coordinate the discovery, verification and remediation of cybersecurity vulnerabilities in critical infrastructure using artificial intelligence tools. Gold Eagle was prompted by Executive Order 14409[1] (Executive Order) signed by President Donald J. Trump on June 2 and backed by several federal agencies. This effort seems to be a direct response to the recent release of powerful new frontier AI models and concerns over how quickly and efficiently they can identify software vulnerabilities that could be exploited by threat actors. In addition to establishing the clearinghouse, the executive order also encouraged advanced AI developers to give the government early access to their models' capabilities to help identify vulnerabilities and directed the federal government to expand access to AI-enabled cyber tools for state and local governments and critical infrastructure operators.

The agencies will partner with open-source software maintainers, AI developers and critical infrastructure operators to 1) aggregate vulnerability findings into a single coordination pipeline and 2) develop and prioritize actionable guidance to remediate those vulnerabilities.

It is still unknown which private companies are involved with Gold Eagle. While participation is voluntary, the goal is tighter coordination between government and industry on AI-related and AI-assisted cybersecurity issues. The clearinghouse will create a more efficient pipeline for identifying and publishing information about open-source software vulnerabilities from a variety of sources, potentially compressing existing patch-management timelines. The Cybersecurity and Infrastructure Agency (CISA)[2] has separately revised its remediation guidance to require fixes for information security systems in federal civilian agencies within a range of three to 60 days, depending on severity. Additionally, critical infrastructure operators may see new, faster-moving channels for receiving prioritized vulnerability and remediation information from CISA and other federal agencies involved in Gold Eagle.

Recommended Next Steps

While information about Gold Eagle is still forthcoming, organizations should consider taking the following steps:

- Federal civilian agencies should review current vulnerability disclosure and patch management timelines against CISA’s updated remediation windows.
- Open-source software maintainers, AI developers and critical infrastructure operators should:

- Monitor forthcoming guidance on Gold Eagle's operational and data-governance framework, including any agency designated to administer the program.
- Assess whether voluntary participation or data-sharing with Gold Eagle would be appropriate and what contractual or confidentiality safeguards would need to be addressed before doing so. Organizations will want to consider whether:
  - They have any disclosure restrictions among customers and third parties that would hinder sharing of information.
  - They will be prepared to meet accelerated timelines for patching vulnerabilities.
  - They are protected from legal liability for the sharing of potential threats and vulnerabilities, particularly since the authorization for the Cybersecurity Information Sharing Act of 2015, which permits and encourages certain disclosures, expires Sept. 30.
- Confirm points of contact with CISA to ensure they are positioned to receive prioritized alerts if and when Gold Eagle begins broader distribution.

The Paul Hastings Data Privacy and Cybersecurity practice regularly advises on security matters and are closely monitoring developments related to Gold Eagle. If you have any questions concerning how Gold Eagle may affect your organization, please do not hesitate to contact any member of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
+1-312-499-6016
aaroncharfoos@paulhastings.com

Dallas

Michelle A. Reed
+1-972-936-7475
michellereed@paulhastings.com

New York

Amir R. Ghavi
+1-212-318-6725
amirghavi@paulhastings.com

Washington, D.C.

Jeremy Berkowitz
+1-202-551-1230
jeremyberkowitz@paulhastings.com

[1] Executive Order 14409, "Promoting Advanced Artificial Intelligence Innovation and Security," "Within 30 days of the date of this order, the Secretary of the Treasury, in consultation with the National Cyber Director, the Secretary of War, through the Director of the National Security Agency (NSA), and the Secretary of Homeland Security, through the Director of CISA, shall form an AI cybersecurity clearinghouse, in voluntary collaboration with the AI industry and operators of critical infrastructure, that coordinates and deconflicts scanning for software vulnerabilities, discovers and validates such vulnerabilities, and coordinates and prioritizes remediation and distribution of vulnerability patches."

[2] CISA is an entity that is part of the Department of Homeland Security responsible for coordinating cybersecurity policy and critical infrastructure protection across federal agencies, state/local governments and the private sector.