ORION FORUM

When AI Finds a Software Flaw, Who Decides When the Affected Vendor Is Told?

SEPTEMBER 14, 2026

In July 2026, the Trump Administration announced GOLD EAGLE, a new federal clearinghouse with the goal of improving cybersecurity vulnerability coordination, using artificial intelligence (AI) to identify software flaws and speed up the time it takes to fix them. While a commendable and necessary effort, the current public details on GOLD EAGLE's design raises several important policy questions. Chief among them and the subject of this analysis: when the clearinghouse takes in a serious, nonpublic flaw (one unknown to the broader security community) who decides whether the affected vendor is notified immediately or if the government can temporarily delay disclosure for intelligence, military, or law-enforcement purposes?

Answering this question requires GOLD EAGLE's routing protocol to be better demarcated than the current public design reveals. To accomplish this, Congress should require GOLD EAGLE to record where all validated, nonpublic findings originated from. Additionally, Congress should establish the presumption that affected vendors are notified immediately and if a federal agency wants to delay notification for some operational purpose, that agency should be required to submit a referral to the Vulnerabilities Equities Process (VEP).

The June 2026 executive order (EO) creating GOLD EAGLE kicked off a thirty-day deadline for the federal government to put together a clearinghouse. Operational since July 2026, the clearinghouse is led by Treasury, with the broad mandate to deconflict scanning, discover and validate vulnerabilities, and coordinate remediation and patch distribution. Other organizations named as partners in the clearinghouse include the Office of the National Cyber Director

(ONCD), the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and leading AI companies and critical infrastructure operators. An August 2026 CISA Fact Sheet directs AI-enabled reporting to the new GOLD EAGLE clearinghouse and keeps the Vulnerability Information and Coordination Environment (VINCE), CISA's primary vulnerability disclosure, available for traditional disclosure. Neither the June EO nor the August Fact Sheet contain the routing protocol for who may delay or disclose decisions for findings once they reach GOLD EAGLE.

Clearly understanding the routing protocol for GOLD EAGLE matters because GOLD EAGLE can receive the same technical fact through a number of different pathways. Take the example of a remotely exploitable flaw present in a network appliance with wide use. An industry partner submits it via the clearinghouse. Later that same day, an independent researcher reports that exact same flaw through an ordinary coordinated disclosure process, under the assumption that the affected vendor will be immediately notified. The next day, a completely different third company shares the same flaw under a nondisclosure agreement. And, finally, after all that other disclosure, a federal scanning team independently reports that same finding, duplicating an outside report, but seeing an operational value in the finding. Across all reporters and report pathways, the vulnerability finding is the same. What differs? The government's authority, the expectation of the reporter, and the appropriate disclosure channel. With no public framework to sort them, the most restrictive handling is likely to win.

The 2017 Vulnerabilities Equities Process (VEP) charter is a framework already in use to help guide federal agencies through the decision to disclose or temporarily restrict new, nonpublic vulnerabilities. VEP's default setting is disclosure, unless an agency can demonstrate a countervailing national security, intelligence, or law-enforcement interest that justifies holding back. It also makes the distinction that vulnerabilities found through security research or incident response and intended for rapid disclosure are out of scope for VEP.

Borrowing from that VEP distinction, the majority of outside submissions should stay within an ordinary coordinated disclosure process, like CISA's previously mentioned VINCE. Meanwhile, the GOLD EAGLE clearinghouse can confirm the report, address any duplication issues, and manage the remediation. If a federal agency wants to delay vendor notification because the flaw has some operational value, that determination should trigger VEP, not be decided in some informal workflow. Within the VEP framework, competing interests can be weighed across agencies and the decision is recorded.

One step in the right direction, the Senate Intelligence Committee's fiscal 2027 authorization bill, addresses weaknesses within AI systems, but fails to establish a process for AI-discovered flaws. It also unacceptably leaves the consultation of key GOLD EAGLE civilian agencies like Treasury, CISA and ONCD, completely up to NSA's discretion. Concurrently, the House bill text as it publicly stands today doesn't contain any matching GOLD EAGLE or AI-found vulnerability provisions. This is a major gap.

Congress can fill it. First, by requiring the clearinghouse to record the origin and handling status of each confirmed, nonpublic finding submitted to it. The record should collect five data points: the source's category (so anonymity is still allowed); which disclosure channel applies; which federal office has responsibility; whether an existing agreement limits or delays sharing; and note if the finding was sent to VEP. The totals drawn from that record should be made available to the public and the Director of National Intelligence's existing annual VEP unclassified reporting appendix should separately publish the referral counts that originate here.

Next, Congress should create a presumption of immediate, coordinated vendor disclosure for all outside submissions. Creating just the presumption here is the correct move, as a default requirement for disclosure would remove all ability for GOLD EAGLE to delay a notification. If a federal agency wants to delay or temporarily restrict a vendor disclosure for an intelligence purpose, then the agency should be required to submit it to the VEP within a short but designated timeframe.

Adoption of these rules would help clarify where GOLD EAGLE ends and the VEP begins. Vendors and researchers should be able understand the reporting paths and where they lead, and Congress and the public should have the information needed to perform appropriate oversight. These additional rules help get us there and should be adopted.

Disclaimer: *Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional policy positions. Accordingly, all views, positions, and conclusions represented herein should be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.*