wiley

ALERT

New AI Incident Reporting Program Proposed for DOD

June 2, 2026

WHAT: A first-of-its-kind program for reporting, tracking, analyzing, and remediating artificial intelligence (AI) incidents and vulnerabilities within the U.S. Department of Defense (DOD) has been proposed by the House Armed Services Cyber, Information Technologies, and Innovation Subcommittee (CITI) for the draft FY2027 National Defense Authorization Act (NDAA), H.R. 8800. The proposal includes provisions for protected disclosures, though other details remain vague. These measures reflect growing congressional focus on ensuring visibility, accountability, and risk mitigation as DOD rapidly expands its use of AI across operations.

WHEN: The Chairman's mark and the CITI print were released May 27, 2026. The Armed Services Committee will mark up the legislation on June 4, and amendments will be posted on the Committee website here.

WHY THIS MATTERS TO INDUSTRY: The draft provisions would direct DOD to create a centralized program for reporting, tracking, analysis, and remediation of "covered AI incidents" and "covered AI vulnerabilities arising from the development, testing, procurement, fielding, or operation" of AI systems. The proposal is notable because no federal program currently exists to comprehensively monitor AI incidents or AI vulnerability reporting, positioning this measure as a potentially significant milestone in federal AI governance, if enacted. The proposal also comes at a time when the federal government is rapidly expanding use of AI in its operations and looking at new ways to address AI procurement, including revising federal guidance on AI last year (covered here) and considering terms and conditions for AI procurement (such as GSA contract terms we covered here). The National Institute of Standards and Technology (NIST) is also

Authors

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Erin M. Joe
Special Counsel
202.719.3140
ejoe@wiley.law

Lauren N. Lerman
Associate
202.719.4664
llerman@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

AI Executive Order
Artificial Intelligence (AI)
Compliance
Cyber and Privacy Investigations, Incidents & Enforcement
Emerging Technologies
Government Contracts
National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology
Trump Administration Resource Center

exploring workstreams to update to existing guidelines and develop of new recommendations for addressing AI incidents as mandated by the Trump Administration's AI Action Plan.

Proposed AI Incident and Vulnerability Reporting Program

The proposed program would provide guidance for the development, testing, procurement, fielding, or operation of AI systems within the DOD, to include a mechanism for DOD and contractor personnel to report certain covered AI incidents and vulnerabilities.

- A "covered AI incident" would include events where an AI system causes or could foreseeably cause unintended harm, operates outside approved guardrails, or materially degrades performance. While "AI system" is not defined in the draft, the proposal incorporates the definition of "artificial intelligence" laid out in 15 U.S.C. § 9401.
- A "covered AI vulnerability" would include any exploitable weakness or systemic issue that could materially affect mission performance, compromise integrity, create safety risks, or result in unauthorized behavior.

Under the CITI draft, the Secretary of Defense would designate an official to manage the program's reporting, tracking, analysis, and remediation of covered AI incidents. While it is unclear who all may be required to report covered AI incidents and vulnerabilities, the program envisions that DOD would create a process for protected disclosures made by members of the Armed Forces, civilian employees, federal contractors, and subcontractors at any tier. That process would include procedures to protect sensitive, proprietary, and classified information submitted through the protected disclosure process.

The provision emphasizes reporting in "good faith" and is designed to encourage participation by prioritizing non-punitive reporting, protection of sensitive and proprietary information, and dissemination of lessons learned. Even so, the draft language may offer less security than contractors may hope for, promising only that "a person making a report in good faith … is not, on the basis of that report alone, subject to adverse contract action … ."

Key Takeaways

DOD seeks additional visibility into AI development. The proposed AI incident and vulnerability reporting program is intended to provide DOD leadership with increased visibility into how AI systems are functioning, including the identification of systemic risks, recurring issues, and necessary corrective actions. The reporting program borrows from existing cybersecurity and vulnerability disclosure programs in offering a protected disclosure process and considering protections for sensitive information, but the definitions of covered AI incidents and vulnerabilities are incredibly broad and reach beyond cyber incidents to encompass other "harms" that are not defined in the proposal.

Additional compliance burdens may impact pace of AI development. The creation of a centralized AI reporting and disclosure program – particularly one coupled with whistleblower protections – could have a significant impact on the pace and manner of AI adoption within DOD. If enacted, one can imagine that AI

contractors may be more hesitant to share AI models in progress with the government if those models are subject to broad reporting of vulnerabilities.

DOD would remain a leader in federal AI adoption. The initiative may serve as a model for other federal agencies to evaluate AI development and operation, particularly as the government continues to scale its use of AI technologies. DOD emerged last year with some of the most driven AI adoption approaches in response to Executive Order 14179, and in January 2026 released the Secretary's Artificial Intelligence Strategy memorandum – and the CITI draft includes another proposal for an AI model "Rapid Deployment Framework" for DOD.

All in all, the CITI proposal signals a major step toward formalizing AI risk oversight within the federal government, combining incident reporting, vulnerability management, and protected disclosure into a unified framework. Contractors and stakeholders supporting DOD AI efforts should monitor these developments closely, as they may introduce new compliance expectations or complicate reporting obligations. Wiley's Privacy, Cyber & Data Governance and Government Contracts practices continue to track these developments. Please reach out to the authors with any questions.