INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

ISOO Notice 2026-01: Responsible Use of Classified National Security Information and Controlled Unclassified Information with Artificial Intelligence

March 30, 2026

Purpose and Background

1. The pace of technological advancement in artificial intelligence (AI) – and its adoption across the federal government – continue to accelerate, often faster than the speed at which guidance, governance structures, and risk-management policies can be developed.

2. In accordance with Presidential direction requiring and encouraging agencies to harness AI's transformative capabilities, it remains essential to both leverage this new capability to further our national security and economic competitiveness as well as pair this innovation with clear, responsible guardrails.

3. In furtherance of this Administration's objectives and policy direction to rapidly and responsibly utilize AI's immense potential, this Notice provides guidance regarding agency handling of classified national security information (classified information) and controlled unclassified information (CUI) with the use of various AI systems and tools.

Responsibilities

4. Pursuant to Executive Order 13526, sections 5.1(a)(1) and (2), and 5.2(b)(1) and (2), the Director of the Information Security Oversight Office (ISOO) is responsible for establishing standards for classification, declassification, and marking principles; safeguarding classified information; develop[ing] directives for the implementation of the order; and for overseeing agency actions to ensure compliance with the executive order and its implementing directives.

5. Pursuant to Executive Order 13556, sections 2(c) and 4(b), the National Archives and Records Administration (NARA)/ISOO serves as Executive Agent of the national Controlled Unclassified Information program and oversees agency actions to ensure compliance, as well as developing and issuing such directives as are necessary to implement the order.

Guidance

6. Executive Order 13526, Classified National Security Information, and Executive Order 13556, Controlled Unclassified Information, govern how classified information and controlled unclassified information must be handled, in tandem with their implementing regulations at 32 CFR 2001 and 32 CFR 2002. Specifically, Part 4 of Executive Order 13526 and 32 CFR §§ 2001.40-2001.55 govern the safeguarding of classified information and stipulate the safeguarding and access requirements. 32 CFR §§ 2002.14 and 2002.16 stipulate the safeguarding, access, and dissemination requirements for CUI. All requirements contained in both executive orders and both federal regulations must be adhered to when considering the proper handling of both types of information on AI systems and in related risk management decisions.

7. If an AI system is Internet-enabled, connected to infrastructure that is external to the agency's control, or otherwise connected to environments that are not accredited for the handling of classified information or that meet the standards for protection of CUI, it is prohibited for agency personnel to input classified information or CUI on such systems.

8. When considering whether classified information or CUI should be permitted on an AI system, it is critical to assess the nature of the AI system of concern. We advise that your agency's chief information officer, chief information security officer, CUI program manager, classification management staff, and information technology staff be involved in such dialogue, in order to fully understand the technical capabilities, limitations, and risk associated with an AI system, as well as the policies and requirements governing classified information and CUI. Agencies should ensure that both their classified information policies and CUI policies are updated to include such guidance. OMB Circular A-11 (2025) requires that agencies budget for any remaining development costs for internal agency policies to phase-in and transition to the CUI program, including costs for lower-level office policies or component agency policies.

9. There are several common types of AI systems. While the definitions of these systems continue to evolve given the rapid pace of development of the AI technologies at their core, it is helpful to understand some of the primary differences between them for the purpose of this Notice and for the dialogues referred to in section 8 above:

> *AI System*: As described in NIST's Artificial Intelligence Risk Management Framework (AI RMF 1.0), an AI system is an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.

Generative AI System: A generative AI system is a form of artificial intelligence that produces new, original content such as text, images, audio, music, or code in response to user inputs.

Open AI System: An open AI system is designed to interact dynamically with its environment. It can receive new inputs, adapt behavior based on external signals, and may evolve over time as a result of these activities. Key characteristics of open AI systems often include external interaction (e.g., continuously ingesting data from users, sensors, or other systems), adaptability (e.g., may update outputs or internal parameters based on new information), non-deterministic behavior (e.g., outputs might change over time even for similar inputs), and feedback loops (e.g., user behavior and real-world events may influence future system behavior). Common examples of open AI systems include conversational assistants or chatbots that learn from usage patterns and user inputs, autonomous vehicles responding to real-time data, recommendation engines that adjust to user behavior, and fraud detection systems that "learn" from emerging threats and new data.

Closed AI System: A closed AI system operates within a fixed, predefined boundary that once deployed, its logic and behavior do not change unless explicitly modified by developers or administrators. Key characteristics of closed AI systems often include no environmental learning (e.g., does not adapt based on new external data), a stationary model (e.g., output is consistent for identical inputs), deterministic behavior (e.g., the output can largely be known in advance), and controlled inputs (e.g., it operates based only on data at the time of creation or deployment). Common examples of closed AI systems include pre-trained models with no updates or periodic planned updates, rule-based expert systems, and other tools with locked logic.

Asymmetric Open/Closed AI System: An asymmetric open/closed AI system, sometimes referred to as a one-way open AI system, is often designed to be open on the inbound side (e.g., the AI can consume broad, external, or continuously updated information), but is closed on the outbound side (e.g., information provided by the user is not used or disseminated further by the system beyond your session or control boundary established by the system's administrator). This type of system is common in regulated deployments as it better enables the protection of data and information provided by the user, while still learning from external sources such as public web data, licensed datasets, periodically refreshed knowledge bases, and/or controlled inputs.

10. Agencies will understandably seek to derive maximum value from AI systems' ability to manage and manipulate organizational information at scale in new and novel ways. At the same time, agencies must ensure, as they enable expanded use of AI systems to meet

their mission objectives, that these systems properly account for and comply with the authorities and requirements governing classified information and CUI.

Authorities

Executive Order 13526, Classified National Security Information.

32 Code of Federal Regulations (CFR) 2001, Classified National Security Information.

Executive Order 13556, Controlled Unclassified Information.

32 CFR 2002, Controlled Unclassified Information.

Executive Order 13690, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government.

Executive Order 14179, Removing Barriers to American Leadership in Artificial Intelligence.

OMB Memorandum 25-21, Accelerating Federal use of AI through Innovation, Governance, and Public Trust.

OMB Memorandum 25-22, Driving Efficient Acquisition of Artificial Intelligence in Government.

America's AI Action Plan, Executive Office of the President, Office of Science and Technology Policy, July 2025.

National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (AI RMF), (www.nist.gov/itl/ai-risk-management-framework).

The National Institute of Standards and Technology Cybersecurity Framework (CSF) 2.0, CSWP 29, The NIST Cybersecurity Framework (CSF) 2.0 | CSRC.

Please direct any questions regarding this ISOO Notice to: isoo@nara.gov.

MICHAEL D. THOMAS

Director