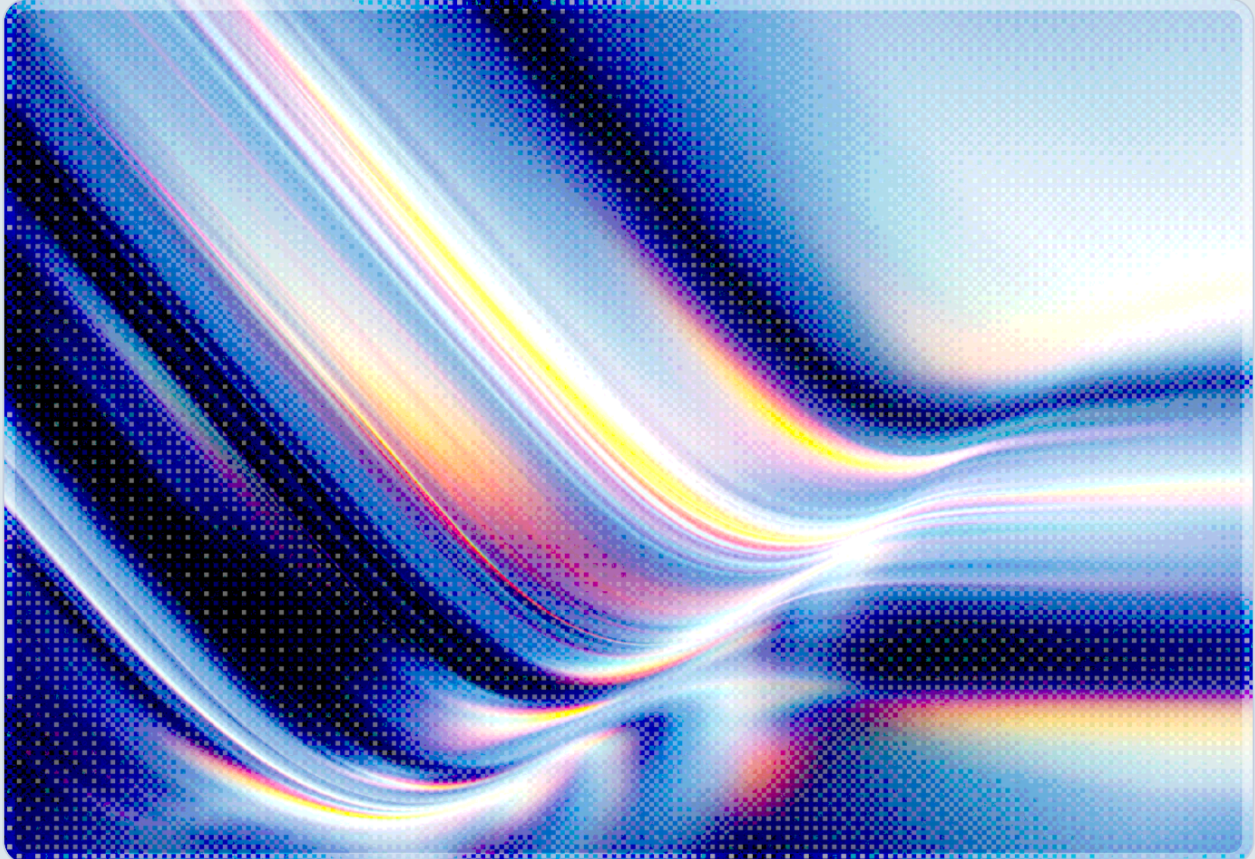


EO 14434 and CAISSI: Mostly a Rebrand, With One Provision to Watch

What the 'Super Intelligence' Terminology Order Changes, and Doesn't, for AI Governance Programs

2026-10-07

 AI-assisted Rapid Research



CSAI

cloud
security
alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

Executive Order 14434, signed September 29, 2026, directs executive branch agencies to use "Super Intelligence" and "SI" in place of "Artificial Intelligence" and "AI" in non-statutory communications. It contains no security, safety, or compliance requirements for the private sector [1]. The order defines the new terms by reference to the existing statutory definition of "artificial intelligence" at 15 U.S.C. § 9401(3), so on its face it creates no new legal category and does not alter existing regulations, contracts, or grants [1][2].

NIST's website now describes the Center for Advancing Innovation and Standards for Super Intelligence (CAISSI), which an independent tracking site reports was previously the Center for AI Standards and Innovation (CAISI) [3][7]. We have not found a separate NIST or Commerce announcement of the change. If the rename is accurate, it is the third public name for the institution in roughly three years [5].

The provision most likely to have substantive consequences is Section 3(b), which directs a 60-day process to propose a statutory definition of "Super Intelligence." A definition that diverges from 15 U.S.C. § 9401(3) could change which systems federal programs cover [1]. Governance programs should therefore avoid rewriting control frameworks around the new vocabulary. They should add a terminology crosswalk, keep legal and contractual references anchored to each instrument's own language, and watch the definition proposal.

Background

On September 29, 2026, the President signed Executive Order 14434, "Inaugurating the Era of Super Intelligence," which the Federal Register published on October 2, 2026 [1]. Section 1 of the order states that current frontier systems "increasingly represent not merely artificial intelligence, but a new era of Super Intelligence," and sets a policy that the executive branch will use the terms "Super Intelligence" and "SI" in place of "Artificial Intelligence" and "AI" to the maximum extent permitted by law. The policy statement adds that the executive branch "will not acknowledge the usage" of the older terms "in any applicable setting" [1]. The order is a terminology directive. It does not establish a program, fund an activity, or impose an obligation on any party outside the executive branch.

Section 2 of the order sets the implementation scope. Agencies are to use the new terms in "official correspondence, public communications, websites, reports, policy documents, and other non-statutory documents within the executive branch," and Section 2(b) states that nothing in the section requires altering previously issued regulations, Presidential actions, contracts, grants, or other historical documents [1]. Section 3(a) defines "Super Intelligence" and "SI" as the technologies and systems encompassed by "artificial intelligence" as defined in 15 U.S.C. § 9401(3), the definition from the National Artificial Intelligence Initiative Act of 2020 [1][4]. That definition governs implementation of the order until superseded by later Presidential action or an Act of Congress. Section 4 preserves agency authorities, makes implementation subject to applicable law and appropriations, and disclaims any enforceable right against the United States [1].

The one forward-looking provision is Section 3(b). Within 60 days of the order, which falls on or about November 28, 2026, the Assistant to the President for Science and Technology must submit proposed legislative language to establish a federal definition of "Super Intelligence." The proposal must include an assessment of whether the definition should "modify, expand upon, or otherwise supersede" the statutory definition of AI, conforming amendments to existing statutory references, and recommendations for further executive action [1]. The order therefore leaves open the possibility that the terminology change will later be paired with a substantive definitional change. As of this writing, no such proposal has been published.

The order lands on an institution that has already been renamed more than once. The U.S. AI Safety Institute was created following the October 2023 executive order on AI, and in June 2025 Commerce Secretary Howard Lutnick announced it would become the Center for AI Standards and Innovation, dropping "safety" from its name [5]. In May 2026, the related AI Safety Institute Consortium was renamed the NIST AI Consortium, a change CSA analyzed at the time [6]. NIST's current Super Intelligence page identifies CAISSI as one of the vehicles through which NIST conducts this work and lists the AI Risk Management Framework among its topic areas [3][12]. The same page describes NIST's output as "voluntary guidelines, tools and other resources" and as support for voluntary, market-driven international standards [3].

The CAISI-to-CAISSI change itself rests on thin sourcing. The NIST page names CAISSI but does not mention CAISI or a rename. The "previously CAISI" lineage comes from an independent tracking site, which states that it is not affiliated with NIST or any government agency and which reported the change on October 1, 2026 [7]. We have not located a separate NIST or Commerce announcement describing the rename or any change to the center's mandate, and NIST news items published through September still use the CAISI name. Readers should treat the rename as reflected on NIST's website but not yet formally explained.

Security Analysis

What the order changes

The direct operational effect falls on federal agencies and, through them, on anyone who produces or consumes federal documents. Agency websites, guidance, and public communications will increasingly say "Super Intelligence" or "SI." Search terms, document titles, and URLs for NIST and other federal resources may change or redirect, which affects any internal tooling that scrapes, indexes, or links to federal AI guidance. Teams that maintain regulatory-tracking systems keyed to the string "AI" in agency publications may see missed matches or noisy results. These are maintenance costs that will vary with how much tooling depends on that string.

A second effect is communicative. The order's language frames frontier systems in terms of "promise" and "limitless opportunities," and it follows a sequence of federal actions that CSA has previously read as shifting institutional emphasis from safety toward standards and innovation [1][6]. We cannot determine from the text whether the terminology change is intended to signal further policy movement. Organizations should treat any inference about future enforcement posture as speculation until agency actions say otherwise. The order itself does not touch the sector-specific rules, procurement requirements, or enforcement authorities that currently shape enterprise obligations.

What the order does not change

The order does not alter any statute. Because the new terms are defined by reference to 15 U.S.C. § 9401(3), regulations, state laws, and contracts that use the term "artificial intelligence" retain their existing meaning [1][4]. The order also does not bind state governments, courts, foreign regulators, or private parties. The EU AI Act, state-level AI statutes, and sector regulators' guidance continue to use their own terminology and definitions, so a multinational governance program will need to operate with at least two vocabularies for the foreseeable future.

The order does not revise NIST's voluntary frameworks on its face. NIST's page continues to list the AI Risk Management Framework under its Super Intelligence topics, and nothing in the order directs NIST to reissue the framework or its profiles [1][3]. Federal obligations enacted earlier in 2026, including those arising from Executive Order 14409 on AI cybersecurity, are likewise unaffected by the order's text, since Section 2(b) leaves previously issued Presidential actions and regulations unchanged [1][8]. Organizations that mapped their programs to those requirements should not need to remap them because of this order.

Nor does the order establish a "Super Intelligence" capability threshold. Some commentary has asked whether SI denotes a more capable class of system than AI. The operative text answers this directly: SI means the same technologies encompassed by the statutory AI definition, and Section 3(b) explicitly separates any capability-based definition into a future legislative proposal [1]. A governance program should therefore not create a separate risk tier called "SI" in response to this order. Doing so would imply a legal distinction that does not currently exist.

Where residual risk sits

Residual risk comes from three sources, the first of which is definitional drift. If the Section 3(b) proposal recommends a definition that expands on or supersedes 15 U.S.C. § 9401(3), then statutory references, federal program eligibility, and procurement language could eventually shift. An expanded definition could sweep in systems that organizations do not currently classify as AI. A narrowed definition, for instance one tied to frontier capability, could remove systems from the scope of federal programs and thereby alter what customers and agencies expect from vendors. The proposal is due to the President rather than to the public, so organizations may have limited visibility into its content before legislation is introduced.

The second source is document and contract inconsistency. Federal customers may begin issuing solicitations, guidance, and questionnaires that use "Super Intelligence" or "SI" while the underlying contract vehicles, FAR clauses, and agreements still use "artificial intelligence." Section 2(b) exempts existing contracts from mandatory alteration, but it does not prevent new documents from using the new term [1]. Vendors answering security questionnaires may encounter ambiguity about whether an "SI system" differs from an "AI system." Our recommendation is to resolve such ambiguity in writing at the time of the engagement, anchored to the statutory definition.

The third source is institutional continuity. Repeated renaming of the NIST center and its consortium, combined with the unclear documentation for CAISSI, makes it harder for enterprises to determine which body owns which workstream, such as agent security standards, evaluations, or measurement science [6][7]. CSA's earlier analysis of the consortium rebrand identified a governance gap, in which no single federal body clearly covers the full range of risks previously addressed under the Safety Institute [6]. A further rename does not change that analysis, but it adds to the verification burden for programs that cite specific federal bodies as authorities.

The table below consolidates the order's effects by area, with the supporting section of the order or source for each.

Area	Effect of EO 14434	Basis
Federal agency communications	Must use "Super Intelligence"/"SI" to the extent permitted by law	EO §2(a) [1]
Existing regulations, contracts, grants	Not required to change	EO §2(b) [1]
Statutory definition	Unchanged; SI is defined as 15 U.S.C. § 9401(3) AI	EO §3(a) [1][4]
Future definition	Legislative proposal due within 60 days	EO §3(b) [1]
Private-sector obligations	None created	EO §4(c) [1]
NIST AI RMF	Continues to be listed by NIST; no stated revision	NIST page [3]
CAISI naming	Center page now reads CAISSI; no separate announcement located	NIST page [3]; independent report [7]

Recommendations

The recommendations below follow from the distinction drawn above between the order's terminology provisions, which require little from private organizations, and its definitional provision, which warrants monitoring. They are grouped by time horizon, beginning with low-effort actions that protect existing references and ending with a view on how to anchor governance programs against future renames.

Immediate Actions

Organizations should confirm that no governance control, policy, or contractual commitment depends on the literal word "AI" in a federal source in a way the rename could break. In practice, this means checking internal links to NIST and other agency pages, updating automated regulatory-monitoring queries to include "Super Intelligence," "SI," "CAISSI," and the prior names, and recording the rename in the program's change log so that auditors can follow references to the new pages. Teams should also confirm that policy citations to NIST resources point to stable, versioned documents rather than to landing pages whose titles may change.

Governance owners should issue a short internal statement that EO 14434 does not change the organization's classification scheme, risk tiers, or control obligations. This statement should state that the organization continues to use "AI" in its own policies, with a crosswalk noting that federal documents may use "Super Intelligence" or "SI" for the same technologies per Section 3(a) of the order [1]. A brief, explicit position prevents business units and vendors from inventing separate "SI" categories on their own.

Short-Term Mitigations

Over the next 60 to 90 days, program owners should add a terminology crosswalk to their policy library and vendor questionnaires, and should define the terms by reference to the statutory definition when responding to federal customers. Vendor contracts and security addenda should keep the defined term the parties already use. For new federal engagements, and with legal counsel, the engagement letter should state that "Super Intelligence" or "SI" in agency documents is read as equivalent to "artificial intelligence" under 15 U.S.C. § 9401(3) unless the agency states otherwise [1][4].

Organizations with federal exposure should assign someone to track the Section 3(b) proposal and any resulting legislative text. Tracking should cover the White House Office of Science and Technology Policy, the Federal Register, and congressional bill text. When a proposed definition appears, the program should run an impact assessment against its AI inventory to identify which systems would gain or lose coverage. Programs should also continue to follow the substantive NIST work that has not changed, including the AI RMF and agent-related standards activities, and verify through NIST's own pages which unit now owns each workstream [3][6].

Strategic Considerations

The broader lesson of this order is that federal terminology is an unstable anchor for enterprise governance. Between 2023 and 2026, the same institution has carried three public names, and the associated consortium has carried at least two [5][6][7]. Programs that anchor controls to risk outcomes, such as model integrity, data protection, agent authority limits, and supply chain assurance, are far less likely to be affected by each rename. Programs that anchor to agency names or phrases will require repeated maintenance.

Leaders should also keep the substantive and symbolic questions separate. The order's terminology provisions require no implementation by private organizations; its definitional provision warrants monitoring. The substantive governance questions that confront enterprises, such as agent authorization, vendor assurance, and how much federal evaluation capacity will remain available to them,

are unchanged by it [6]. Organizations should continue to invest in internal continuous risk monitoring and independent third-party assurance rather than assuming that federal naming or institutional changes will either fill or widen governance gaps on their behalf.

CSA Resource Alignment

CSA's most directly relevant prior work is its analysis of the preceding renaming, "NIST Drops Safety From AI Consortium: Implications for Enterprise Governance" [6]. That note established that renaming of federal AI bodies can accompany shifts in emphasis, and it recommended that enterprises treat NIST AI RMF 1.0 [12] as the operational baseline, document naming changes, and build internal continuous-monitoring capability. The present note extends the same reasoning: CAISSI is a further instance of a naming change whose practical effect on enterprise obligations is minimal and whose effect on federal emphasis requires monitoring rather than reaction.

CSA's research on the 2026 Presidential AI executive orders provides the substantive context against which this terminology order should be read. "Executive Order 14409: AI Cybersecurity Deadlines Take Effect" analyzes the AI cybersecurity order's compliance deadlines for federal agencies and critical infrastructure operators [8], and "Federal AI Security Mandates: CISO Action Guide" maps the 2026 AI executive order's voluntary and mandatory elements to enterprise governance frameworks [9]. Those documents describe obligations that remain in force; EO 14434 does not alter them. Readers who need a compliance baseline should use those analyses rather than infer obligations from the terminology order.

For the control structure that should remain stable through terminology change, CSA's AI Controls Matrix (AICM) v1.1 organizes AI-specific controls into a set of control domains that is not tied to any single agency's vocabulary [10]. Mapping a program to AICM and to the NIST AI RMF, rather than to agency-specific wording, is a durable way to absorb future renames. CSA's AI Organizational Responsibilities guidance can be used to ensure ownership of the crosswalk and monitoring tasks described above [11].

References

- [1] The White House / Office of the Federal Register. "[Executive Order 14434 of September 29, 2026: Inaugurating the Era of Super Intelligence](#)." 91 Fed. Reg. 63129, October 2, 2026. Federal Register record: <https://www.federalregister.gov/d/2026-20321>.
- [2] The White House. "[Inaugurating the Era of Super Intelligence](#)." Presidential Actions, September 29, 2026.
- [3] NIST. "[Super Intelligence](#)." National Institute of Standards and Technology, accessed October 7, 2026.
- [4] Legal Information Institute, Cornell Law School. "[15 U.S. Code § 9401 – Definitions](#)." U.S. Code, National Artificial Intelligence Initiative Act of 2020.
- [5] Technical.ly. "[US Dept. of Commerce nixes 'safety' in NIST AI institute](#)." Technical.ly, June 2025.
- [6] Cloud Security Alliance. "[NIST Drops Safety From AI Consortium: Implications for Enterprise Governance](#)." CSA AI Safety Initiative, May 2026.
- [7] USASI (independent project, not affiliated with NIST or any government agency). "[NIST adopts 'super intelligence' wording and introduces its CAISSI center page](#)." October 1, 2026.
- [8] Cloud Security Alliance. "[Executive Order 14409: AI Cybersecurity Deadlines Take Effect](#)." CSA AI Safety Initiative, July 2026.
- [9] Cloud Security Alliance. "[Federal AI Security Mandates: CISO Action Guide](#)." CSA AI Safety Initiative, 2026.
- [10] Cloud Security Alliance. "[AI Controls Matrix \(AICM\)](#)." Cloud Security Alliance, v1.1.
- [11] Cloud Security Alliance. "[AI Organizational Responsibilities: Core Security Responsibilities](#)." Cloud Security Alliance.
- [12] NIST. "[AI Risk Management Framework](#)." National Institute of Standards and Technology.