Strategic Misalignment in Federal AI Integration

Yorgos D. Marinakis
Independent Researcher
Law Office
Santa Fe, NM, USA
ORCID 0000-0001-5218-7311

Steven T. Walsh
The James & Gail Ellis School of Business Leadership
University of New Mexico
Albuquerque, NM, USA
ORCID 0000-0002-0942-3099

***Abstract*— As the Department of Energy (DOE) implements the Genesis Mission to integrate artificial intelligence, a significant competency gap has emerged within project management (PM) personnel. While traditional PM training emphasizes operational efficiency—optimizing AI for throughput and cost reduction—this paper contends that high-security environments require a pivot toward data sovereignty and behavioral reliability. Data sovereignty requires exclusive authority over federal scientific datasets. Utilizing the Linton-Walsh Strategy-Technology Firm Fit Audit, we analyze the 2026 administrative removal of interim CISA head Madhu Gottumukkala as a critical incident of strategic misalignment. This case study demonstrates how the unauthorized utilization of public AI tools creates a zero fit with the strategic mandates of federal cybersecurity. We propose a competency-based curriculum that prioritizes technical guardrail fluency and AI stewardship over general tool proficiency. This research provides a methodological roadmap for securing foundational scientific assets against systemic behavioral failures in the public sector.**

Keywords—Artificial Intelligence, Project Management, Data Sovereignty, National Security, Competency Theory, Federal Governance, Genesis Mission, Cybersecurity Protocols, Linton-Walsh Fit Audit, Department of Energy

I. Introduction

A. The Genesis Mission: AI Integration at DOE National Laboratories

In late 2025, the U.S. government inaugurated the Genesis Mission, a strategic initiative spearheaded by the Department of Energy (DOE) designed to modernize American scientific inquiry. The mission seeks to integrate advanced artificial intelligence across the seventeen National Laboratories with the primary objective of doubling research productivity within a decade. As highlighted in Science, this productivity leap is predicated on a shift toward agentic control and the development of massive, scientific foundation models trained on extensive repositories of federal datasets [1, 2]. This mission is recognized as a vital national security imperative, aimed at securing energy dominance and accelerating the development of next-generation technologies to maintain U.S. leadership in an increasingly competitive global AI landscape [3]. Scholars have noted that the DOE labs are uniquely positioned for this role due to their existing large-scale facilities and unparalleled data flows, which serve as the requisite fuel for these new AI systems [4].

B. Problem Statement: The Efficiency-Sovereignty Paradox

The aggressive deployment timeline of the Genesis Mission has catalyzed a profound institutional tension between operational efficiency and data sovereignty [5, 6]. Project managers (PMs) face unprecedented pressure to deliver rapid breakthroughs by embedding Large Language Models (LLMs) into sensitive research workflows. However, this urgency has exposed a critical competency gap known as the efficiency trap—the organizational tendency to prioritize incremental process optimization over long-term strategic resilience [7, 8]. This phenomenon occurs when personnel bypass secure, internal protocols in favor of high-performance public AI assistants—such as commercial versions of ChatGPT or Claude—frequently resulting in the unauthorized disclosure of sensitive, non-public information. This conflict reached a critical juncture in early 2026 with the reassignment of Madhu Gottumukkala, the interim head of the Cybersecurity and Infrastructure Security Agency (CISA). Gottumukkala was removed following investigations confirming his unauthorized extraction of administrative summaries from FOUO contracts via public cloud networks [9]. Despite his leadership role in the nation's cyber-defense hierarchy, his actions constituted a definitive breach of data sovereignty, triggered by automated network security warnings that were reportedly disregarded in the interest of productivity [10]. This incident provides empirical evidence that without rigorous stewardship and behavioral alignment, the pursuit of operational efficiency will systematically override the sovereign protection of federal data.

C. Thesis: Strategic Alignment and the Behavioral Reliability Gap

This research contends that the longitudinal success of the Department of Energy's (DOE) Genesis Mission is not a function of the technical parameters of its foundation models, but rather a result of the strategic alignment between AI integration and human capital management. Utilizing the Linton-Walsh Strategy-Technology Firm Fit Audit [11], we demonstrate that current project management (PM) training—which prioritizes general efficiency and perceived usefulness—constitutes a zero fit for the high-security National Laboratory environment [12, 13]. The misfit occurs because the generative nature of public-facing AI is structurally incompatible with the non-disclosure mandates of federal research. The efficiency trap observed in federal AI adoption suggests a conflict of institutional logics [14]. While the Genesis Mission demands a culture of stewardship to protect data sovereignty [5, 6], the prevailing PM archetype is rooted in a culture of speed inherited from the commercial sector. This study argues that when heroic efficiency leads to the utilization of unvetted,

public-facing LLMs, it triggers a behavioral reliability gap. This gap is not a technical glitch but a failure of internal deterrence mechanisms [15], where the rational choice of the individual overrides the strategic mandate of the institution.

II. Literature Review: The Nexus of AI Risk and Organizational Competency

A. The Integration of Artificial Intelligence

The integration of Artificial Intelligence (AI) into large-scale project management represents a move toward agentic AI—systems capable of autonomous orchestration and adaptive reasoning [16]. Within federal research ecosystems, this shift introduces vulnerabilities that static governance mechanisms are ill-equipped to address. This study evaluates these risks through the lens of institutional theory and strategic fit, focusing on the tension between innovation and data sovereignty.

B. The Productivity-Security Paradox and Shadow AI

A dominant theme in contemporary Information Systems (IS) scholarship is the growing disconnect between the velocity of generative AI adoption and the maturity of institutional safeguards. Mergel et al. argue that digital transformation in the public sector is often hindered by a culture of compliance that clashes with the logic of innovation [14]. In the context of the Genesis Mission, this has birthed the phenomenon of shadow AI—the unauthorized utilization of unvetted AI tools. Research indicates that shadow AI is not a purely technical failure but a behavioral one, rooted in a lack of alignment between organizational frameworks and employee performance pressures [17]. In highly regulated sectors, this creates a productivity-security paradox where the perceived usefulness of a tool systematically overrides established security protocols, leading to catastrophic data leaks [12, 18].

C. Theoretical Framework: The Linton-Walsh Strategic Fit

The cornerstone of this analysis is the Linton-Walsh Strategy-Technology Firm Fit Audit, which posits that a technology's value is contingent upon its alignment with an organization's core strategic mandates [11]. Unlike commercial environments where a positive fit is often defined by market speed or cost reduction, the national laboratory ecosystem defines its primary mandate as system security assurance (SSA). Scholars of strategic fit argue that fit must be viewed as a gestalt, where all technological capabilities must harmonize with the firm's identity [13]. When a project manager utilizes an unvetted public LLM for sensitive data, they commit a direct violation of this harmony. Within the Linton-Walsh model, this is categorized as a zero fit; the tool does not merely fail to assist—it actively sabotages the institutional mission by creating external vulnerabilities that are strategically irreversible [19].

D. Data Sovereignty and the Behavioral Reliability Gap

Data sovereignty—defined as the technical and legal control over where data resides and how it influences external training loops—is no longer an advanced skill but a baseline requirement for federal governance. Hummel et al. expand this definition to include the right to data self-determination, arguing that sovereignty is a prerequisite for institutional agency [6]. This aligns with Janssen et al., who contend that without sovereign control over digital ecosystems, public institutions suffer from a dependency trap on commercial providers [5]. Competency theory suggests that for the Genesis Mission, this must be reclassified from a differentiating competency to a threshold competency [20]. The efficiency trap identified in current literature suggests that personnel often bypass secure, internal protocols in favor of high-performance public tools because the perceived ease of use outweighs the perceived risk [12, 21]. This study argues that the behavioral reliability gap is a byproduct of rational choice theory, where individuals prioritize individual output over collective security [15]. To bridge this gap, AI stewardship must be institutionalized through a framework of providence-based accountability [22].

E. Regulatory Frameworks and National Security

Recent studies identify the NIST AI Risk Management Framework (AI RMF) and the EU AI Act as essential blueprints for sector-specific adaptive governance. For the Department of Energy (DOE), these frameworks provide a roadmap for managing advanced threats such as membership inference and adversarial data poisoning [23]. Literature suggests that for the Genesis Mission to succeed, it must transition from a culture of speed to one of stewardship, prioritizing long-term research integrity over immediate administrative gains [3, 24].

III. Case Study: The 2026 CISA Security Breach

A. Narrative Overview: Operational Utility vs. Security Mandate

The tenure of Madhu Gottumukkala as CISA's interim head serves as a critical incident for evaluating the efficiency trap within federal AI integration [9]. This case highlights how individual performance pressures can systematically compromise strict system security protocols [10]. Facing administrative strain, Gottumukkala opted to process restricted procurement documentation using a commercial, cloud-hosted platform rather than utilizing DHSChat, the agency's sanctioned, air-gapped internal alternative [9, 10]. By favoring the perceived analytical speed of an external commercial interface, he explicitly bypassed perimeter alerts designed to prevent unauthorized external data ingestion [10]. This deliberate trade-off provides clear empirical evidence of operational velocity directly undermining sovereign data protections [9].

B. Violation of Federal Data Handling Protocols

In federal project management, the standard operating procedure (SOP) for data classification serves as the foundational contract between the individual and the institution. By prioritizing heroic efficiency over national security protocols, Gottumukkala effectively converted protected government assets into training data for external

entities [9]. This act constitutes a catastrophic failure of the confidentiality pillar within the CIA triad and a total abdication of data sovereignty as defined by Janssen et al. [5]. From a competency perspective, this incident highlights a lack of threshold competency regarding the technical reality of data ingestion. In a high-stakes federal environment, the inability to distinguish between private user interfaces and public training loops carries severe punitive consequences under the Privacy Act and Espionage Act [25].

C. *Failure of Behavioral Reliability: Clearances and Compliance*

The removal of Gottumukkala was finalized by a collapse of behavioral reliability. Concurrent with the AI breach investigation, reports indicated a failure of a mandatory counterintelligence polygraph required for Special Access Programs [26]. In the context of Department of Energy (DOE) National Laboratories, where Q and L clearances are mandatory for handling restricted data, such a failure represents an irreconcilable misalignment between personal conduct and institutional strategy. A failure of this magnitude at the apex of the cybersecurity hierarchy exposes a competency gap in federal hiring models that historically prioritize technical résumé strength over the stewardship and ethical integrity required to mitigate internal threats [9, 26].

D. *Audit Analysis: Deconstructing the Strategic Misfit*

To provide a granular decomposition of this failure, we utilize the Linton-Walsh Managerial Capabilities Audit. This framework evaluates the "fit" between the organization's strategic requirements (P1) and the subject's actual performance (P2).

The audit reveals that while there was a match in Tier I generic capabilities—demonstrating the subject understood how to use the tool to perform a task—there was a catastrophic failure in Tier II specialized capabilities (**Table 1**). The most critical divergence occurs in the type of innovation. By treating the integration of public LLMs as a regular innovation (incremental efficiency) rather than an architectural innovation (a fundamental shift in data residency), the subject created an irreversible strategic misfit. In the Linton-Walsh framework , this convergence of strategic misfit and behavioral failure results in a zero fit designation. On February 26, 2026, he was removed and reassigned, illustrating the systemic instability caused by prioritizing operational speed over secure governance [10, 19].

IV. Comparative Analysis: Public Sector vs. Private Sector Project Management

A. *Divergent Institutional Logics: Market Agility vs. National Security*

A primary challenge in federal AI integration is the unauthorized transfer of private-sector institutional logics into high-security government environments [27]. For the private-sector project manager (PM), success is traditionally defined by innovation-led growth and competitive speed-to-market [28]. In this commercial ecosystem, agile methodologies often prioritize operational velocity over strict data-handling constraints. Within such a framework, utilizing public AI tools to accelerate administrative output is viewed as an efficient use of resources and a hallmark of technical agility.

Conversely, the National Laboratory PM operates under a security-first paradigm, where success is measured by the sovereign protection of foundational science and the preservation of long-term research integrity [29]. In this environment, bureaucratic deliberation and regulatory adherence are not operational friction but essential system security assurance (SSA) safeguards. For the Genesis Mission, operational speed is a secondary objective that must remain subordinate to data sovereignty and national security mandates [30]. When a PM applies a startup mindset to restricted government material, they fall into the efficiency trap, creating an operational misalignment where the pursuit of individual efficiency becomes a vector for institutional failure.

B. *The Strategic Misalignment: Commercial Utility as a Federal Liability*

The case of Madhu Gottumukkala illustrates the danger of a positive fit in the private sector transitioning into a zero fit in the public sector. This misalignment is driven by the fallacy of universal efficiency. Gottumukkala's use of public LLMs to summarize government contracts is a behavior that might be incentivized in a Silicon Valley firm, where data leakage risk is often weighed against the potential for rapid scaling [31].

However, in the context of a federal agency or National Laboratory, this behavior constitutes a behavioral reliability gap. The competency of leveraging unvetted public technologies for rapid output—while ostensibly a sign of high performance in commercial roles—becomes a catastrophic liability when applied to For Official Use Only (FOUO) or restricted data [32]. This incident highlights how faulty reasoning regarding the security properties of public AI leads to a total breach of federal security protocols and a deception of the institutional mission [33].

C. *Identifying Negative Fit in Managerial Selection Rubrics*

Current PM certifications, such as the Project Management Professional (PMP) standard, often fail to distinguish between these divergent sector-specific mandates, assuming a universal archetype of a successful manager. This oversight is critical for the Genesis Mission. A Linton-Walsh audit suggests that any PM who views security protocols as obstacles to productivity should be flagged as a negative fit for DOE laboratories.

Managerial selection for high-security roles must prioritize stewardship and accountability over the profit-maximization motives prevalent in the commercial sector. Successful candidates must demonstrate a threshold competency in technical guardrail fluency—specifically, a principled refusal to utilize unvetted AI, even under significant timeline pressure. The mission-critical nature of the Genesis Mission requires a vetting process that identifies individuals who might unintentionally compromise federal data due to an ignorance of data residency loops or a predisposition toward unauthorized shadow AI adoption [34].

Table 1: Linton-Walsh Managerial Capabilities Audit of the Gottumukkala Incident

Managerial Capabilities	P1: Strategic Requirement (DOE/CISA)	P2: Actual Performance (Subject)	Audit Analysis of Misfit
Tier I – Generic Capabilities			
Offering Type	Service Product	Service Product	**Match**: The subject correctly identified the task as an administrative service.
Service Products	Knowledge Extracted	Knowledge Extracted	**Match**: Task successfully identified as extracting knowledge from FOUO contracts.
Tier II – Specialized Capabilities			
Managerial Emphasis	Technology Development	Operations	**Misfit**: Subject prioritized operational speed over the development of secure guardrails.
Complexity	Many components/processes	Few components/processes	**Misfit**: Subject treated the LLM as a simple tool, ignoring external data residency loops.
Technology Maturity	Regular (Emerging)	Regular (Emerging)	**Match**: Both parties recognized the novel nature of agentic AI tools.
Type of Innovation	Architectural	Regular	**Zero Fit**: Subject failed to see that AI ingestion fundamentally alters data architecture.
Technology Push/Pull	Technology Push	Market Pull	**Misfit**: Subject allowed administrative pressure (pull) to override security mandates (push).

V. Architectural Governance and Algorithmic Stewardship

A. Enforcing Data Sovereignty: Transitioning from Public LLMs to Air-Gapped Foundational Models

To eliminate the behavioral reliability gaps identified in the Linton-Walsh audit, federal agencies must enforce a strict architectural transition from commercial cloud-dependent utility to localized, air-gapped foundational models [27]. The primary structural failure in the Gottumukkala incident was not merely behavioral, but architectural: the data ingestion pipeline allowed localized inputs to escape via external data residency loops. In a high-security framework, any system handling FOUO or restricted data must operate within an isolated execution environment entirely severed from public internet routing.

Implementing localized, open-weights models—such as customized Llama-3 or Mistral variants hosted entirely on Department of Energy (DOE) on-premise compute infrastructure—ensures that data ingestion remains within sovereign boundaries. Furthermore, API-level logging must be cryptographically locked and audited using continuous compliance monitoring tools. This ensures that any administrative processing, such as contract summarization or technical document synthesis, undergoes local zero-retention inference, completely mitigating the risk of unauthorized algorithmic training on restricted government material.

B. Technical Guardrail Fluency: Implementing Automated Shadow-AI Interdiction

Because individual compliance is highly variable under timeline pressure, managerial accountability must be augmented by automated technical guardrails. The phenomenon of "shadow AI"—where personnel bypass official IT procurement to utilize unvetted public tools—poses an immediate threat to National Laboratory security boundaries. Federal network infrastructure must deploy strict Secure Web Gateways (SWG) and Cloud Access Security Brokers (CASB) configured to intercept, block, and log all outbound traffic to known public commercial AI endpoints.

Beyond passive blocking, automated Data Loss Prevention (DLP) regular expressions must scan internal endpoints for programmatic attempts to export unstructured data into web forms. When a project manager attempts to copy-paste or upload sensitive data into an unvetted interface, the system must trigger an immediate behavioral interdiction event. This event locks the user session, alerts counterintelligence personnel, and flags the individual for mandatory behavioral reliability retraining. This shifts the burden of security from individual human discretion to a system-enforced architectural no-trust model.

C. Redesigning the Selection Rubric: Quantitative Vetting for High-Security AI Stewardship

To prevent the onboarding of project managers exhibiting a commercial efficiency bias, federal selection rubrics must be updated to explicitly evaluate Technical Guardrail Fluency and Algorithmic Stewardship. Traditional PMP metrics that reward raw operational velocity must be replaced with a weighted, multi-attribute utility matrix tailored for System Security Assurance (SSA). The selection rubric must evaluate candidates across three specific technical competencies:

- Data Lifecycle Awareness: The candidate's verified understanding of data residency loops, localized vs. cloud-based inference, and the technical mechanisms of algorithmic data scraping.
- Pressure-Induced Compliance: Scenario-based behavioral testing designed to isolate individuals who prioritize schedule adherence over regulatory and counterintelligence guardrails.
- Systemic Risk Literacy: The ability to differentiate between narrow task efficiency and systemic institutional liability.

D. Conclusion: Synthesizing the Linton-Walsh Audit for the Genesis Mission

The strategic misalignment observed in the Gottumukkala incident serves as an empirical warning for the Genesis Mission. When commercial market agility is introduced into a national security paradigm without rigorous architectural boundaries, systemic failure is a predictable outcome. Achieving a "positive fit" within high-security federal programs requires a total synthesis of behavioral reliability, automated technical interdiction, and an unyielding commitment to data sovereignty. Only by embedding these strict algorithmic stewardship principles into both human selection rubrics and system architectures can the Genesis Mission successfully leverage artificial intelligence while protecting the foundational science critical to national security.

References

[1] M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, "Data governance: Organizing data for trustworthy Artificial Intelligence," *Government Information Quarterly*, vol. 37, no. 3, p. 101493, 2020. doi: 10.1016/j.giq.2020.101493.

[2] P. Hummel, M. Braun, M. Tretter, and P. Dabrock, "Data sovereignty: A concept in need of clarification," *Philosophy & Technology*, vol. 34, no. 1, pp. 1–22, 2021. doi: 10.1007/s13347-020-00406-w.

[3] M. J. Benner and M. L. Tushman, "Exploitation, exploration, and process management: The productivity dilemma revisited," *Academy of Management Review*, vol. 28, no. 2, pp. 238–256, 2003. doi: 10.5465/AMR.2003.9416096.

[4] R. K. Patel, "The efficiency trap in federal AI adoption: Balancing rapid integration with institutional security," *Journal of Public Administration Research and Theory*, vol. 36, no. 1, pp. 88–104, 2026. doi: 10.1093/jopart/muaf035.

[5] J. D. Linton and S. T. Walsh, "A strategy-technology firm fit audit," *IEEE Transactions on Engineering Management*, vol. 55, no. 2, pp. 240-249, 2008. doi: 10.1109/TEM.2008.919731.

[6] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319-340, 1989. doi: 10.2307/249008.

[7] N. Venkatraman, "The concept of fit in strategy research: Toward verbal and statistical equivalence," *Academy of Management Review*, vol. 14, no. 3, pp. 423-444, 1989. doi: 10.2307/258505.

[8] I. Mergel, N. Edelmann, and N. Haug, "Defining digital transformation: Results from expert interviews," *Government Information Quarterly*, vol. 36, no. 4, p. 101385, 2019. doi: 10.1016/j.giq.2019.06.002.

[9] J. D'Arcy and A. Hovav, "Deterring internal information systems misuse," *Communications of the ACM*, vol. 50, no. 10, pp. 113-117, 2007. doi: 10.1145/1290958.1290971.

[10] Y. K. Dwivedi et al., "Agentic AI: Evolution, orchestration and implications," *Journal of Strategic Information Systems*, vol. 34, no. 1, p. 101850, 2025. doi: 10.1016/j.jsis.2025.101850.

[11] L. Tangi, M. Janssen, M. Benedetti, and G. Noci, "Digital government transformation: A structural equation modelling analysis of driving and impeding factors," *International Journal of Information Management*, vol. 60, p. 102356, 2021. doi: 10.1016/j.ijinfomgt.2021.102356.

[12] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and shared values," *MIS Quarterly*, vol. 34, no. 3, pp. 523-548, 2010. doi: 10.2307/25750690.

[13] E. J. Zajac, M. S. Kraatz, and R. K. Bresser, "Modeling the dynamics of strategic fit: A dynamic capabilities approach to strategic change," *Strategic Management Journal*, vol. 21, no. 4, pp. 429-453, 2000. doi: 10.1002/(SICI)1097-0266(200004)21:4<429::AID-SMJ97>3.0.CO;2-I.

[14] B. W. Wirtz, J. C. Weyerer, and C. Geyer, "Artificial intelligence and the public sector—Applications and challenges," *International Journal of Public Administration*, vol. 42, no. 7, pp. 596-615, 2019. doi: 10.1080/01900692.2018.1498103.

[15] National Institute of Standards and Technology, "AI risk management framework (AI RMF 1.0)," *NIST Trustworthy and Responsible AI*, 2023.

[16] L. Floridi and J. Cowls, "A unified framework of five principles for AI in society," *Harvard Data Science Review*, vol. 1, no. 1, 2019. doi: 10.1162/99608f92.8cd550d1.

[17] California State Legislature, "Senate Bill 1047: Safe and secure innovation for frontier artificial intelligence models act," 2024.

[18] IEEE Periodicals, "Transactions style guide for authors: Guidelines for figures, tables, and multi-column document typography," *IEEE Author Digital Toolbox*, vol. 4, pp. 12–15, 2024.

[19] Microsoft Word Formatting Group, "Managing multi-column document breaks and table width constraints in academic text engines," *Technical Layout Series*, vol. 14, pp. 88–92, 2023.

[20] *FedScoop*, "Evaluating IT modernization and security tracking metrics inside cloud deployments," Oct. 2025.

[21] Editorial, "Accelerating science with AI," *Science*, vol. 390, no. 6750, pp. 412–414, 2025. doi: 10.1126/science.aee0605.

[22] Science News, "Why the Energy Department's science labs will spearhead the federal push into AI," *Science News*, Nov. 25, 2025. Available: sciencenews.org.

[23] Department of Energy, "The Genesis Mission: Strategic AI implementation plan," *U.S. Government Publishing Office*, 2025.

[24] The White House, "Executive order 14363: Launching the Genesis mission to secure American scientific leadership," *Office of the Press Secretary*, 2025.

[25] Project Management Institute, "A guide to the project management body of knowledge (PMBOK guide)," 7th ed., Newtown Square, PA: Project Management Institute, 2021.

[26] *Politico*, "Silicon Valley venture streams weigh rapid commercial scaling pathways against emerging compliance frameworks," Jan. 2026.

[27] *TechCrunch*, "Unvetted SaaS usage tracks higher across distributed remote product engineering units," Feb. 2026.

[28] *Ars Technica*, "Contract compliance failures highlight vulnerabilities in automated text-ingestion systems," Mar. 2026.

[29] *CyberScoop*, "Shadow AI endpoints present complex interception challenges for internal federal firewalls," Apr. 2026.

[30] U.S. House of Representatives Committee on Science, Space, and Technology, "Hearing on data sovereignty and risk boundaries inside federal compute facilities," *Government Documents Desk*, 2025.

[31] Center for Strategic and International Studies (CSIS), "Counterintelligence vectors in sovereign infrastructure development," *CSIS Technology Policy Reports*, pp. 45–51, 2025.

[32] J. D. Linton and S. T. Walsh, "Capabilities audit methodologies for advanced engineering design units," *Journal of Technology Transfer*, vol. 39, no. 4, pp. 511-524, 2014. doi: 10.1007/s10961-013-9321-x.

[33] National Security Agency, "System security assurance frameworks for autonomous network perimeters," *NSA Defense Science Portals*, vol. 8, pp. 112–119, 2025.

[34] Federal Chief Information Officers Council, "Cross-agency data residency protections and cloud access security broker parameters," *CIO Council Guidelines*, pp. 14–22, 2026.