carahsoft.
TECHNOLOGY BY POLICY

Intelligence Authorization Act FY26

Division F of the National Defense Authorization Act

December 18, 2025

Overview

The Intelligence Authorization Act (IAA) dictates how the U.S. Intelligence Community (IC) will govern, adopt, and scale technology as a core mission capability in FY26. Through Title LXVI and Subtitle C, it establishes enforceable requirements for AI governance and security, risk-based testing, interoperability and data-rights-focused procurement, standardized technology adoption metrics, coordinated intelligence sharing on emerging technologies, and resilient infrastructure planning. For government and industry, the IAA shifts technology from experimentation to enterprise-level, measurable, and secure deployment, directly shaping IT budgets, acquisition priorities, and vendor requirements across classified environments.

What is the Intelligence Authorization Act?

The Intelligence Authorization Act, or Division F of the National Defense Authorization Act (NDAA), provides statutory direction for how the IC governs, oversees, and executes its missions in FY26. In recent years, the IAA treats technology as a core mission enabler, establishing requirements for AI governance, cybersecurity, data sharing, interoperability, performance measurement, and resilient infrastructure across classified environments. The IAA directly shapes IC IT budgets, procurement expectations, security and testing standards, and modernization priorities, influencing which technologies agencies adopt, how vendors compete and are selected, and how solutions must be designed, secured, evaluated, and scaled across the IC.

TITLE LXVI—ARTIFICIAL INTELLIGENCE AND OTHER EMERGING TECHNOLOGIES

Title LXVI - Artificial Intelligence and Other Emerging Technologies establishes the Intelligence Community's formal governance framework for AI and other advanced technologies, translating policy priorities into enforceable IT requirements. It drives standardized AI security guidance, risk-based testing and evaluation, Chief Artificial Intelligence Officer (CAIO) oversight, and stronger procurement rules around interoperability, data rights, model reuse, and supply-chain security. For industry, Title LXVI signals increased demand for secure, interoperable, and governable AI and software solutions that can operate in classified environments, support measurable performance and trust standards, and withstand heightened scrutiny of foreign technology risk.

Section	Mandates
Sec. 6601 - Artificial Intelligence Security Guidance	• NSA must issue and update AI security guidance to counter nation-state theft, sabotage, and supply-chain risks • Requires identification of AI vulnerabilities and high-risk lifecycle points • Mandates strategies for AI systems to identify, protect, detect, respond, and recover from cyber threats • Allows collaboration with government, research, and private-sector partners on AI safety and security

Sec. 6602 - AI Development and Usage by the Intelligence Community	• Establishes CAIOs across all IC elements to oversee AI governance • Requires IC CIO & IC CAIO to identify reusable AI systems/functions within **1 year** • Directs IC elements to share custom AI code, models, and model weights where feasible • Requires model contract terms supporting data rights, interoperability, and competition • Mandates performance evaluation of all IC AI systems for safety, fairness, transparency, and trustworthiness
Sec. 6603 - Application of AI Policies to Publicly Available Models in Classified Environments	• Applies IC AI governance policies to publicly available AI models used in classified systems • Requires risk-based testing standards, benchmarks, and secure testing environments for model evaluation • Prohibits the IC from directing vendors to alter models to favor a specific viewpoint • Requires DNI to update IC AI policies as needed
Sec. 6604 - Prohibition on Use of DeepSeek	• Mandates removal of DeepSeek and successor applications from IC national security systems • DNI must issue removal standards within **60 days** of enactment • Requirements must align with federal information security standards • Allows limited national security and research exceptions with risk-mitigation measures

SUBTITLE C—OTHER MATTERS

Subtitle C-Other Matters focuses on execution, accountability, and infrastructure resilience that directly affects technology adoption across the IC. It requires common metrics to measure the operational impact of emerging technologies, mandates rapid coordination and intelligence sharing on critical and emerging tech across agencies, and advances planning for resilient energy infrastructure to support mission-critical IT systems. For industry, Subtitle C reinforces a shift toward outcome-driven technology adoption, cross-agency standardization, and long-term investment in secure infrastructure, shaping how IT solutions are evaluated, scaled, and sustained across the IC.

Section	Mandates

Sec. 6621 - Enhancing IC Technology Adoption Metrics	• Requires DNI, CIA, NSA, NGA, NRO, and DIA to implement a common set of technology adoption metrics within **270 days**
	• Metrics assess agency-wide adoption, integration, and operational impact of emerging technologies
	• Requires each agency head to brief Congress within one year on:
	  ○ Established metrics
	  ○ Progress against metrics
	  ○ Legislative or regulatory changes needed to improve adoption
	• Applies standardized evaluation across IC elements while allowing agency-specific implementation processes

Sec. 6622 - Report on IC Sites for Advanced Nuclear Technologies	• Requires DNI, in coordination with DoD and DOE, to identify IC sites suitable for advanced nuclear energy deployment within **240 days** • Targets resilient, secure energy solutions for IC facilities with operational or maintenance responsibility

	• Requires deployment plans that:
	  ○ Prioritize early site prep and licensing
	  ○ Aim to begin nuclear deployment within **3 years** of enactment
	  ○ Allow optional interconnection to the commercial grid if it enhances national security
	  ○ Ensure nuclear fuel is free from international regulatory obligations
	• Expands long-term energy resilience for mission-critical IT and facilities

Sec. 6623 - Strategy on Intelligence Coordination for Critical & Emerging Technologies	• Requires DNI to develop an IC-wide intelligence coordination strategy within **60 days**
	• Covers collection, processing, analysis, and dissemination of foreign intelligence on critical and emerging technologies
	• Mandates structured intelligence sharing with civilian agencies responsible for:
	  ○ Regulation and standards
	  ○ R&D and innovation
	  ○ Science and public health
	  ○ Export controls, screening, and financial tools
	• Requires submission of the strategy to Congress within **30 days** of completion

Important Deadlines

Deadline	Mandate
60 Days (Feb 16, 2026)	IC-wide emerging technology sharing strategy (Sec. 6623)
60 Days (Feb 16, 2026)	DeepSeek removal standards (Sec. 6604)
240 Days (Aug 5, 2026)	Nuclear site identification report (Sec. 6622)
270 Days (Sep 13, 2026)	Tech adoption metrics implemented (Sec. 6621)
1 Year (Dec 18, 2026)	AI reuse identification & Congressional metric briefing (Sec. 6602 / 6621)
3 Years (Dec 18, 2028)	Begin nuclear deployment at IC sites (Sec. 6622)

What Does This Mean for Government?

These provisions push the Intelligence Community toward more disciplined, enterprise-level technology management, particularly regarding AI and emerging technologies. Agencies must move faster from experimentation to operational use while applying consistent security, testing, and performance standards across classified environments. Leadership accountability increases through CAIO roles, standardized adoption metrics, and required reporting to Congress, while coordination requirements reduce duplication across IC elements. Overall, the IAA forces the government to treat AI, software, data, and infrastructure as mission systems with clear governance, measurable outcomes, and resilient, secure foundations.

What Does This Mean for Industry?

For vendors, solutions must support risk-based testing, transparent performance metrics, data and model portability, and strong supply-chain assurances to compete in IC procurements. Preference will increasingly flow to technologies that integrate cleanly into classified environments and can scale across multiple agencies through reuse and standard interfaces. Best positioned vendors are FedRAMP-aligned, security by design, and willing to align contracts and architectures with IC data-rights and lifecycle oversight expectations.