AI Governance in National Security

As artificial intelligence (AI) becomes increasingly central to national security operations, effective AI governance frameworks are essential for responsible development and deployment at scale. AI governance provides the structure necessary to ensure AI systems align with legal, ethical, and operational requirements while maintaining public trust and mission effectiveness. This primer explores the key aspects of AI governance that national security practitioners need to understand to effectively manage AI initiatives within their organizations.

Why AI Governance Matters

AI governance provides the guardrails and processes needed to:

1. Align AI systems with democratic values, legal requirements, and agency mission

AI systems must operate within existing legal frameworks while upholding democratic values. For the defense and intelligence community, this means ensuring AI applications comply with established authorities including the Privacy Act, Foreign Intelligence Surveillance Act (FISA), Law of Armed Conflict, US DoD Code 3000.09 (Autonomy in Weapon Systems), and agency-specific directives such as the Intelligence Community Directive 203.

AI systems must align with core principles such as privacy preservation, fairness, consideration of human rights, operational reliability, and resilience against adversarial actions. In national security applications, AI governance must also address additional considerations, such as the protection of classified information, rules governing the use of force, joint-force interoperability, and the geopolitical implications of AI deployment including risks of escalation by adversaries.

2. Maintain Justified Confidence in System Performance

Confidence in AI system performance is paramount in national security contexts. This requires:

- Demonstrated technical reliability through rigorous testing and validation
- Transparent decision-making processes that can be audited when necessary
- Designing for human-AI collaboration, which includes built-in interpretability features that allow operators to understand system outputs
- Proven resilience against adversarial attacks and manipulation attempts
- Risk-proportionate controls and safeguards

3. Enable Effective Oversight and Accountability

Successful AI governance requires clear organizational structures and processes. Key elements include:

- Defined chains of responsibility, oversight, and accountability
- Mechanisms for identifying and correcting errors
- Standardized evaluation and deployment procedures

Implementation Framework

Implementing AI governance in a department/agency typically follows a four-phase process:

Step	Description	Actions	Examples
1. Principles & Values Setting	Establishing ethical guidelines and core values to align AI with national interests and civil liberties.	- Conduct stakeholder consultations to identify core ethical priorities - Align principles with existing agency authorities and missions	ODNI AI Ethics Principles, DoD AI Ethical Principles, DHS AI Directive
2. Framework Development	Translating principles into actionable guidance to assess, mitigate, and manage risks.	- Map principles to specific operational requirements - Create/ drawn on risk assessment templates and evaluation criteria	ODNI AI Ethics Framework, GSA AI Guide
3. Organizational Structure Setup	Defining roles and responsibilities and establishing oversight bodies to ensure accountability.	- Establish reporting structures and accountability chains - Identify knowledge gaps in staff that requires training	DoD Chief Digital and AI Office (CDAO), Federal Chief AI Officers
4. Operational Implementation	Executing AI policies with clear guidelines, ownership, and evaluation metrics.	- Deploy pilot programs to test governance frameworks - Define KPIs and feedback loops for continuous improvement	DoD Responsible AI Strategy, DHS AI Roadmap, DHS Policy Statement: Acquisition and Use of Artificial Intelligence, State Dept AI Strategy

Common Implementation Challenges

Resource Constraints: Limited availability of AI-skilled personnel and funding can impact governance implementation. Methods to implement governance with minimal initial resources are to start with a single use case, employ pilot programs, or build on existing resources such as the NIST AI Risk Management Framework.

Compliance Burden: Balancing governance requirements with operational efficiency requires careful planning. Focus on streamlining processes where possible while maintaining necessary oversight and controls.

Interoperability: Different systems and agencies, even ones that work very closely together like IC agencies, may use varying standards and approaches. Work to align governance frameworks with partner organizations while maintaining agency-specific requirements.

Key Takeaways for National Security Professionals

- Ensure AI systems comply with existing laws.
- Utilize standardized frameworks such as the NIST AI Risk Management Framework to assess and mitigate risks.
- Establish clear oversight and accountability structures within your agency.
- Stay informed about evolving policies and regulatory changes to anticipate their impact on national security operations.