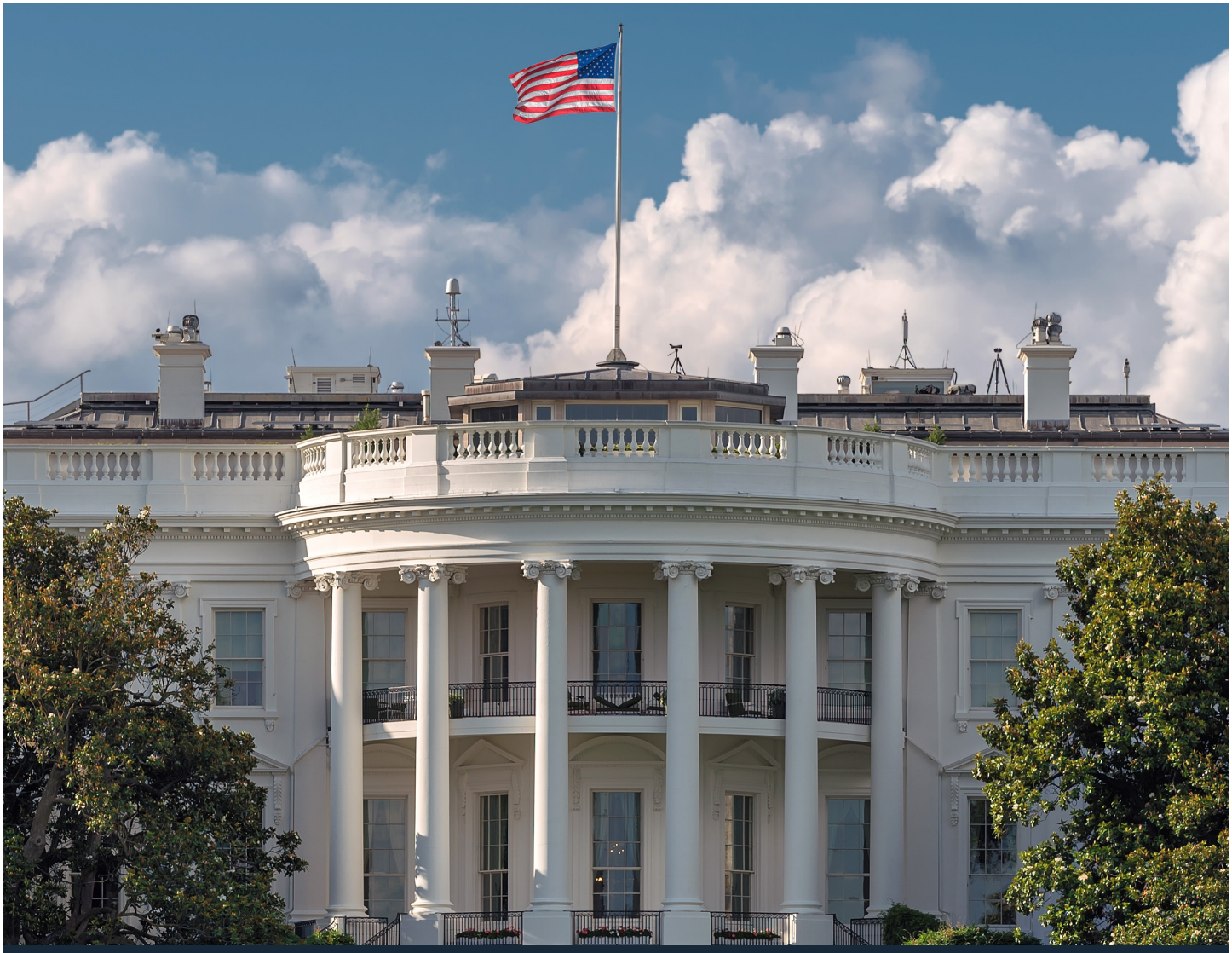


PRESIDENTIAL TRANSITION MEMO

Building a Secure Tomorrow: Strategic Recommendations to Enhance Efficiency and Technical Skill Sets Within the IC

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

INTRODUCTION

As the incoming Administration prepares to take office, addressing the critical issues of technology, innovation, cybersecurity, and the transformative implications of artificial intelligence (AI) within the Intelligence Community must be a priority. While the nation's dedicated intelligence professionals continue to address complex global threats with resilience and expertise, gaps in resources, policies, and procedures hinder mission efficiency and effectiveness. Establishing a framework that promotes innovation, supports sound policy development, and attracts and retains a top-tier workforce is critical to maintaining the United States' competitive edge.

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit membership organization dedicated to advancing public-private-academic partnerships to address critical intelligence and national security priorities. Representing over 175 organizational members, INSA brings together senior leaders and emerging professionals within the public, private, and academic sectors. Our membership includes current and former leaders from the intelligence, military, and government communities, as well as analysts, and experts from industry and academia.

This memo reflects the collective insights of our 10 policy councils, subject matter experts, and thought leaders, who have identified key priorities that merit immediate attention in the Administration's first 100 days. The document outlines preliminary recommendations to guide policy development and operational improvements across two strategic pillars:

I. **Enhancing Efficiency and Capability:** Streamlining security processes and cultivating a leaner, more skilled workforce.

II. **Strengthening Collaboration:** Building robust partnerships between government, industry, and academia to tackle complex intelligence and national security challenges.

These recommendations serve as an initial roadmap, offering actionable guidance to inform both near-term priorities and long-term strategic planning. INSA stands ready to support the Administration by collaborating with government officials, industry leaders, and academic partners to develop innovative, impactful solutions that will strengthen the nation's intelligence and national security mission.

STRATEGIC PILLARS

I. ENHANCING EFFICIENCY AND CAPABILITY

1. Right-Sizing the Force: Cybersecurity and AI Skill Sets

As AI-associated technologies continue to rapidly evolve, the IC must enact policies that promote upskilling to close knowledge gaps. Maintaining technological and capability superiority is vital for current and future operations. The status quo has led to a shortfall of skilled professionals needed to meet the moment. Collaboration with industry leaders and educational institutions will enable the development of targeted training programs to meet cybersecurity skill demands.

Recommendations:

- **Prepare the Workforce for AI Evolution:** Prioritize workforce preparedness by promoting new training and tools and supporting applied research in emerging technologies.
- **Develop AI-Centric Education:** Create and deliver learning modules to provide current IC professionals with foundational and intermediate knowledge of AI's technical and strategic uses. This should include critical thinking skills that prepare the workforce for the impacts of AI-enabled automation, human-machine teaming, bias, and malicious content.
- **Ensure Adequate Funding for Human Capital Research:** Ensure appropriate funding is authorized to support research programs and the required infrastructure necessary for this endeavor. The INSA Foundation's Future of the IC Workforce white paper, released in October 2024, identified closing skill gaps, early STEM education, and cross-sector flexibility as key to attracting and retaining a highly skilled workforce. Critically, this approach provides the opportunity to identify roles and skill sets deemed the most important in support of the IC mission while phasing out others as a part of a larger strategic plan.
- **Launch an IC National Cybersecurity Workforce Initiative:** Focus on attracting and training the next generation of cybersecurity professionals. This should include expanding scholarship programs, apprenticeships, and public-private partnerships. Building on the National Cyber Workforce and Education Strategy, emphasize skills-based hiring and contract reform to create accessible career pathways for individuals who may not have 4-year degrees.

2. Security Policy Reform: Reciprocity and Streamlining the Clearance Process

Trusted Workforce 2.0 is the greatest security transformation in the past 70 years. It is showing steady progress with the completion of all the major policy elements and is on a course correction for the information technology system critical to its successful implementation across the government. The policy forward is clearly in place, but as the program reaches the critical stage of implementation, it will be important for the new Administration to continue pushing forward reform efforts and ensure agency heads adhere to the new guidelines in place. Key components, such as Continuous Vetting, are demonstrating major payoffs in getting people on mission more quickly and identifying issues that can be dealt with earlier.

Recommendation:

- Continue supporting the transformation of the personnel vetting process. Engage HPSCI, SSCI, HASC, and SASC on key initiatives and adopt industry recommendations necessary to maintain progress while identifying more opportunities to streamline systems and create additional efficiencies.

3. Reconceptualize the Sensitive Compartmented Information Facility (SCIF) Workplace

The COVID-19 pandemic demonstrated the IC's ability to adapt to hybrid work models. As employers transition back to the pre-COVID norms, talent acquisition and retention could be impacted, particularly among cleared personnel in which lifestyle flexibility has become not just highly valued but a necessity. This would include new regulations to address cleared personnels' ability to maintain their clearances more efficiently as they transition between the public and private sectors.

Recommendation:

- Ensure the continued recruitment and retention of a highly-skilled, cleared workforce by offering financial incentives for working in a SCIF, upgrade SCIF technology to align with industry standards, expand personal communication zones, standardize reciprocity for medical and fitness devices, and introduce the use of "We-Work" style SCIFs to enhance flexibility and collaboration.

4. Implementation of TEMPEST and ICD 705 Standard

IC and DoD agencies have moved to review legacy SCIF and Security Access Program Facility (SAPF) accreditation decisions. The goal is to bring technical security countermeasures in line with updated standards. However, these updated requirements were not clearly articulated to impacted industry partners. This lack of clarity has imposed significant costs on companies with previously accredited, operational facilities that no longer meet the increased technical security requirements.

Recommendation:

- Ensure that the ODNI asserts oversight for physical and technical security policy, and that the National Counterintelligence and Security Center (NCSC) coordinates the requirements and execution across the defense and intelligence communities. Industry should be included in this process to understand the evolving threat and to develop revised or additional countermeasures strategies that will minimize unnecessary costs and maximize effectiveness.

II. STRENGTHENING COLLABORATION

1. Strengthening Public-Private Partnerships

Public-private partnerships are essential to the IC's success in addressing national security challenges. While some efforts, like NSA's Cybersecurity Collaboration Center, highlight the potential of these partnerships, comprehensive solutions remain underutilized across government.

The private sector often identifies challenges and delivers innovative, cost-effective solutions more quickly than government efforts alone. Additionally, when government officials depart to pursue other opportunities, it is often industry that retains critical expertise and institutional knowledge.

Recommendations:

- Establish a high-level joint task force with equal representation from government and industry. This task force should include representatives from the security, contract, acquisition, and policy arenas, in oder to properly identify and address problems and coordinate both proactive and reactive security responses. This task force should be empowered to rapidly share threat intelligence, coordinate incident response efforts, and develop joint cybersecurity exercises. For example, regular tabletop exercises involving key stakeholders would enhance preparedness and improve response coordination during real-world cyber incidents.
- Collaborate with INSA to advance emerging technologies and cybersecurity priorities by promoting capacity-building exercises, launching joint research initiatives targeting shared threats, and implementing information-sharing frameworks to strengthen national security capabilities.
- Streamline acquisition processes that enable rapid adoption of emerging technologies, to include expanding the use of Other Transaction Authorities (OTAs) and creating dedicated innovation pipelines. This approach will strengthen major system acquisition programs, and aid in acquiring emerging technologies such as AI, quantum computing, and advanced cybersecurity tools. Deeper collaboration between government and industry will ensure a more agile, innovative, and effective approach to safeguarding national security.

2. Enhancing Critical Infrastructure Resilience

Power grids, roadways and railways, air traffic control systems, water systems, and communication networks – among other key resources – are vital to national security. The disruption of these systems through cyber and/or kinetic attacks can weaken the Nation's ability to respond to threats and crises as well as damage our economic interests.

Recommendation:

- Mandate the implementation of Zero Trust Architecture principles across all critical infrastructure sectors. This approach will significantly reduce the attack surface and limit the impact of successful breaches. Additionally, it incentivizes the adoption of advanced cybersecurity technologies like AI-powered threat detection and automation tools to stay ahead of evolving threats. Additionally, consider the adoption of policies that drive preparation due to unforeseen circumstances. For instance, mandating data backups and resilient application architectures to prevent and mitigate critical losses of information.

3. Clarify the Direction of AI in the IC

AI applications for the IC are distinct from the broader national security apparatus, as operational concerns—such as ensuring intelligence quality and upholding tradecraft standards—are paramount. To close this gap, the government must prioritize transparency and accountability while fostering data practices that enhance algorithmic decision-making.

Currently, the U.S. government has few codified principles guiding the use and deployment of AI technologies. This lack of timely and thoughtful governance continues to hinder the Nation's ability to compete, leaving us lagging behind adversaries who are leveraging AI with greater agility and purpose.

Recommendation:

- Prioritize the establishment of clear guidelines, standards, and frameworks for AI development and deployment, tailored specifically to Title 50 operational use cases. These should include enforceable requirements for high-quality training data, robust AI model security, and rigorous testing protocols to identify and mitigate deficiencies. Maintaining human oversight throughout the process is critical. These guidelines must balance innovation with ethical considerations by providing clear rules and guardrails, ensuring the development and use of AI technologies align with national security objectives and operational integrity.

4. Exploitation of Open Source Intelligence (OSINT) and Social Media

In recent years, non-traditional media sources have become pervasive, offering a wealth of verifiable data that can enhance intelligence reporting and analysis on critical topics and priorities. Open-source intelligence (OSINT) presents significant opportunities to streamline processes, making them more timely and relevant. By leveraging OSINT, the IC can accelerate threat identification, verify the current locations of targets and forces, and address a range of other operationally significant tasks.

Recommendation:

- Conduct a review of existing documentation regarding the use of OSINT in support of IC operations. Several strategies already exist at both the ODNI and agency levels. Prioritize efforts to build on this foundation by identifying opportunities to advance OSINT integration, leverage AI tools and other emerging technologies, and address challenges related to cross-domain storage and utilization.

5. Review of Industrial Security Policy

The National Industrial Security Program (NISP), administered by the Defense Counterintelligence and Security Agency (DCSA), oversees the protection of classified U.S. Government information across Government Contractor Activities (GCAs) and provides overarching security policy guidance to cleared and trusted contractors. This program is essential for mitigating threats and securing sensitive government information entrusted to private industry.

Recommendations:

- Ensure the National Industrial Security Program has sufficient resources and personnel to review security specifications, verify and audit contractor clearances, and manage access to classified information for all awarded contracts involving sensitive data.
- Collaborate regularly with DCSA to identify any gaps or shortfalls in the implementation of NISP policies across the government and its growing contractor network. Particular attention should be given to sectors in which emerging technological innovation is outpacing federal government regulation, such as cybersecurity, artificial intelligence, and quantum computing.

CONCLUSION

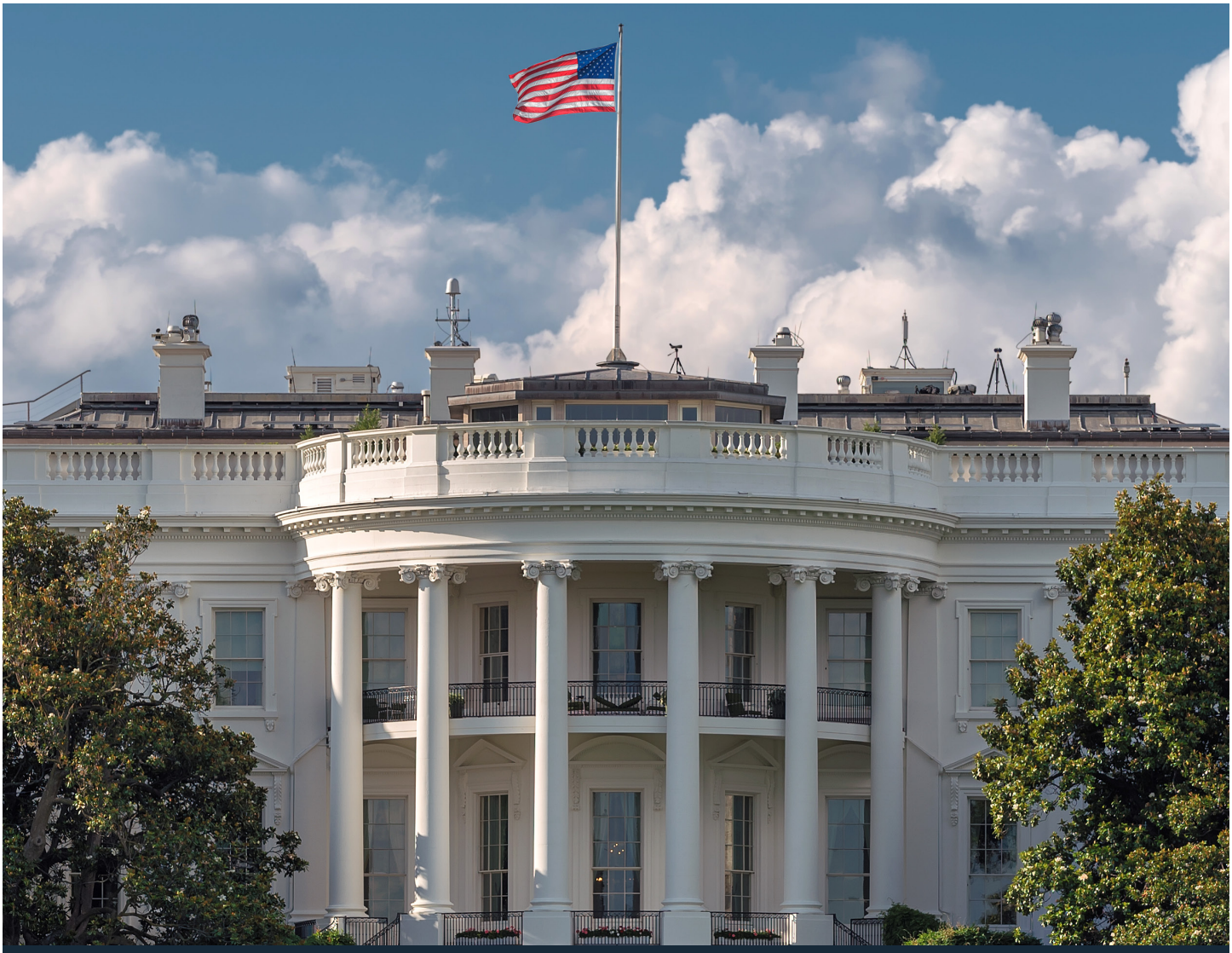
The challenges our nation faces today—ranging from the rise of advanced artificial intelligence to threats against critical infrastructure and the imperative to maintain technological superiority—are both complex and urgent. This memo presents actionable recommendations that align with the Trump Administration's commitment to reducing inefficiencies and delivering meaningful results. By cutting through bureaucratic barriers, strengthening public-private collaboration, and ensuring the delivery of timely, relevant intelligence, this framework aims to foster a secure, innovative, and globally competitive technology ecosystem. These measures will enable a leaner, more agile, and effective intelligence community while safeguarding national interests. Together, we can build a resilient future, leveraging advanced technologies to protect our freedoms, preserve our security, and maintain strategic dominance.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 175+ member organizations and 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

For more information, please contact INSA's policy team at 703-224-4672 or PR@insaonline.org.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE



INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

INSAONLINE.ORG