



Vision for the IC Information Environment

An Information Technology Roadmap

May 2024



FROM THE DNI AND IC CIO



The 2023 National Intelligence Strategy states that the Intelligence Community (IC) faces a different strategic environment from September 2001 when the Nation came under massive attack. The United States now faces determined adversaries of many types—peer countries to non-state actors—seeking to challenge our national interests and our security. Similarly, the information technology (IT) available today is different from 2001.

We rely on IT to enable missions throughout the IC. We operate in an information-rich environment, moving at unprecedented pace to support analysis and collaboration, and enable insights for intelligence consumers and partners. IT must evolve if the United States is to remain strong and safe. Beyond fixing current shortcomings, we must advance our IT until it represents a strategic advantage over our rivals.

The IC needs to embrace new technologies that can reshape the intelligence process and rapidly deliver valuable intelligence to policymakers, operators, and warfighters to remain ahead of those seeking to undermine and threaten the United States and its allies and partners. To that end, more than 100 technical leaders across the IC developed the recommendations contained in this document, arranged into five Focus Areas. We agreed to take bold measures and push our IT to the forefront of better mission capabilities, and to update this Roadmap annually using a similarly collaborative process with IC stakeholders and outside experts to stay current with technological changes and ahead of threats.

This IC-endorsed Roadmap informs future investments and drives intelligence change. The vision is ambitious on purpose. Driving this change will require commitment to necessary shifts in culture; educating the workforce; and recruiting, developing, and retaining talent with needed skillsets. Achieving this vision will require continued partnering with stakeholders in related areas of innovation, AI, and procurement and acquisition.

We thank all the Community Chief Information Officers (CIO), leaders, and subject matter experts who dedicated their time and expertise to identifying these focus areas and initiatives. Together we have the opportunity, the talent, and the determination to close IT gaps and open new mission horizons to secure our country.

A handwritten signature in black ink, appearing to read 'Avril D. Haines', written over a horizontal line.

Avril D. Haines
Director of National Intelligence

A handwritten signature in black ink, appearing to read 'Adele J. Merritt', written over a horizontal line.

Dr. Adele J. Merritt
Intelligence Community CIO

TABLE OF CONTENTS

Introduction	4
Focus Area 1.0: Fortify the Mission with a Reliable and Resilient Digital Foundation	6
Key Initiatives.	7
1.1 Make More World-Class Capabilities Available to Mission by Optimizing the IC's Cloud Environment	7
1.2 Meet the Demands of Tomorrow by Advancing and Scaling Compute, Storage, and Transport.	8
1.3 Enable the Intelligence Mission Anywhere by Empowering the Edge	8
Focus Area 2.0: Assure the Mission with Robust Cybersecurity	9
Key Initiatives.	10
2.1 Protect Our Mission from the Inside Out by Achieving Zero Trust	10
2.2 Deliver the Right IT at the Right Time through Modernized Enterprise Risk Management	11
2.3 Strengthen the IC's Collective Defenses by Maturing and Integrating Security Coordination	11
2.4 Increase Security and Speed of Software Delivery through Development, Security, and Operations (DevSecOps)	12
2.5 Keep Our Most Sensitive Intelligence Safe by Realizing Quantum Resistant (QR) Cryptography	13
2.6 Batten Down the Hatches by Securing/Hardening Cross Domain Solutions (CDS).	13
Focus Area 3.0: Enable the Mission with Modern Practices and Partnerships	14
Key Initiatives.	15
3.1 Connect Our People by Enhancing and Extending Collaboration	15
3.2 Enable Dynamic Information Sharing by Cultivating Agile and Non-Traditional Partnerships	16
3.3 Tap into the Full Power of the IC Talent Pool by Achieving Ubiquitous IT Accessibility	16
3.4 Put the Multi-INT in Intelligence by Advancing Interoperability Among IC Elements	16
Focus Area 4.0: Enhance the Mission with Data-Centricity	17
Key Initiatives.	18
4.1 Expedite Mission Outcomes by Realizing End-to-End Data Management.	18
4.2 Maximize Intelligence Value by Implementing a Data-Centric Architecture	19
4.3 Empower the Analyst by Transitioning Sensitive Data Siloes to Data-Centric Enclaves	19
Focus Area 5.0: Accelerate the Mission with Advanced Technologies and Workforce Readiness	20
Key Initiatives.	21
5.1 Unleash More, Better, Faster by Advancing AI at Scale	21
5.2 Meet the Future When It Arrives by Preparing Now for Over-the-Horizon Capabilities	21
5.3 Capitalize on Tomorrow's Capabilities by Priming the Future Workforce	22
Appendix A: References	23

Introduction

The IC provides the United States and its allies and partners with unmatched decision advantage over adversaries. As an information-driven enterprise, infrastructure underpins success. The IC relies on exquisite IT to execute its missions and produce intelligence for U.S. decision makers. The timeliness and accuracy of the intelligence mission are essential.

To protect our country, the IC must continue to invest in the modernization and hardening of infrastructure. Ensuring analysts have the capability to discover, access, and leverage the IC's data at the speed of mission requires a robust digital foundation with sufficient capacity to scale on demand. This includes flexibility to meet rapidly evolving mission needs to collaborate with partners.

Much of the IC's missions run on unseen IT. This can lead to complacency when it comes to funding important infrastructure investments needed to keep pace with evolving adversary capabilities and tactics. The rapid pace of changing technology further risks the infrastructure stability. The IC must work together to address antiquated systems, processes, and policies; and overcome cultural barriers.

Further, Artificial Intelligence (AI) is poised to transform the IC's mission. Secure, generative, and predictive AI can reduce the time for intelligence insights from days or weeks to mere seconds. However, this AI-driven future depends on a resilient, sound, and secure infrastructure.

At the Director of National Intelligence's request, the IC CIO worked across the Community with CIOs, Chief Architects, Chief Information Security Officer (CISOs), Chief Data Officers (CDOs), the Senior Agency Official for Privacy, and Science and Technology leaders to identify five priority Focus Areas where investment will be most needed in the next five years. These areas are interrelated, interconnected, and interdependent.

This IC-endorsed executive document is designed so that the IC CIO Council can update and validate it annually, and the IC can stay ahead of threats and abreast of rapid technological advancements. To neglect any of the Focus Areas will endanger the IC's future capabilities. The time is now for strategic and substantial investment in the core IT infrastructure of the IC.

The Five Focus areas are:

- **Focus Area 1.0:** Fortify the Mission *with a Reliable and Resilient Digital Foundation* – Maintaining intelligence superiority depends on delivering unique insights from IC elements. Such insights depend on a strong, resilient, and interoperable foundation of network, compute, storage, security, and IT services. Mission success requires essential investment in the underpinning of, and enabling of, the enterprise IT capabilities.
- **Focus Area 2.0:** Assure the Mission *with Robust Cybersecurity* – Modern infrastructures and threats require modern cybersecurity methodologies to create the required agility for success while maintaining enterprise-wide security. Zero Trust (ZT) is central to securing the IC Information Environment (IE).

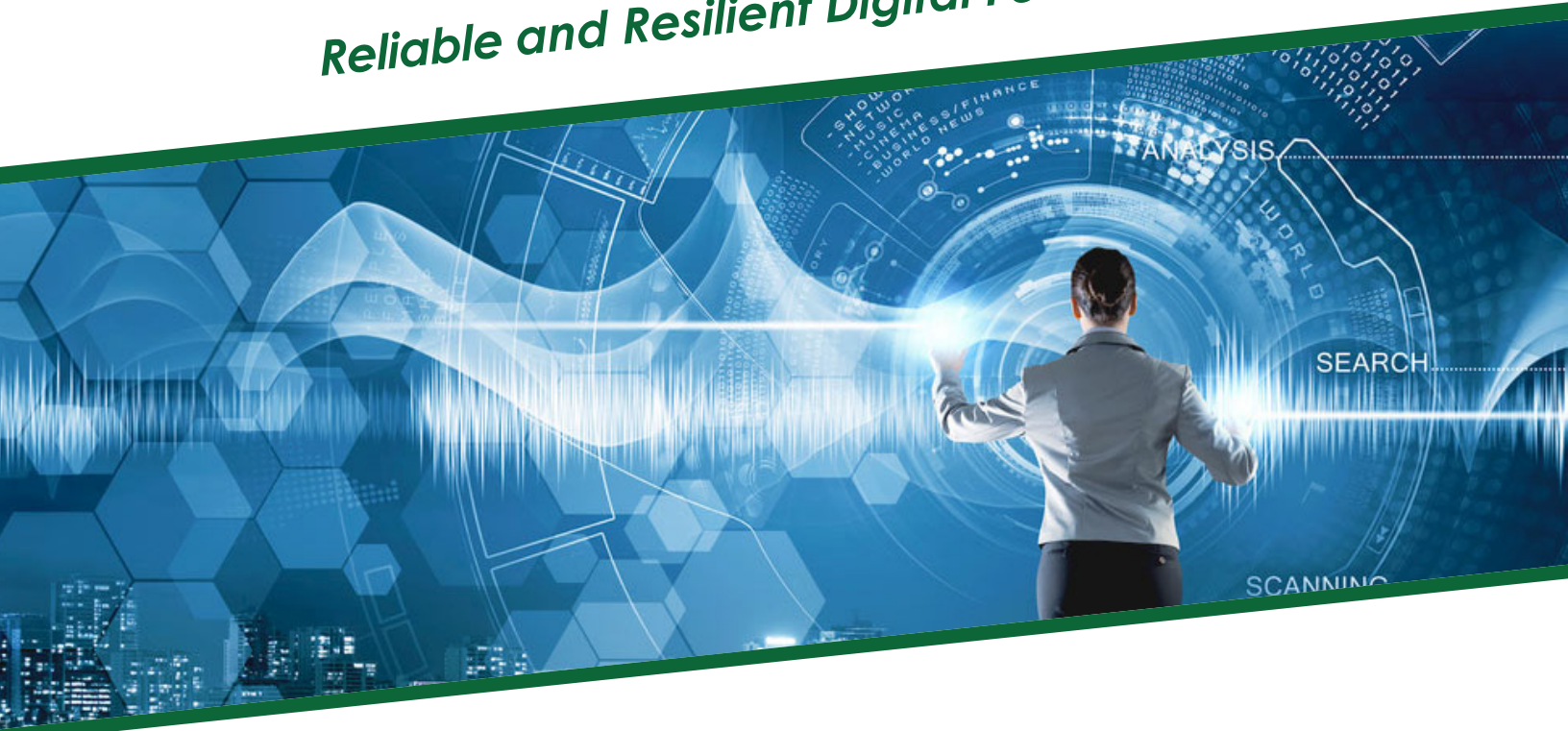
- **Focus Area 3.0:** Enable the Mission *with Modern Practices and Partnerships* – The IC does not succeed in its mission without partners, both internal to the IC and external, including the Department of Defense (DoD); foreign partners; Federal, State, Local, Territorial, and Tribal (FSLTT) government partners; industry; and academia. Likewise, the IC’s future mission success will depend on its ability to remain competitive technologically and ensure technology is accessible to all of its workforce.
- **Focus Area 4.0:** Enhance the Mission *with Data-Centricity* – Timely, accurate, well-informed insight is key to delivering enhanced mission outcomes. The IC must shift from an organization- and system-centric paradigm to one that is data-centric; preserves organizational equities, authorities, and rights; implements legal/compliance frameworks; and enforces security. This is of paramount importance in the next five years if the IC is to position itself to accelerate the mission with AI and other advanced technologies.
- **Focus Area 5.0:** Accelerate the Mission *with Advanced Technologies and Workforce Readiness* – Increased human and machine teaming is the current frontier for intelligence. IC elements will need to pursue the successful delivery and adoption of emerging techniques to assure future mission success. Furthermore, the IC will have to ensure the workforce is ready to meet the future when it arrives.

This document builds on, reflects, and is mutually-reinforcing of major IC strategies as well as those in development (see Appendix A, “References”). This vision is not an implementation plan and does not mandate IC element action. Rather, the recommended Key Initiatives and Target Milestones within this document will provide senior stakeholders the insights necessary to make strategic decisions that close IT gaps and lead the IC into a future that continues to deliver unrivaled advantage for the United States and its allies.



Focus Area 1.0


Fortify the Mission with a Reliable and Resilient Digital Foundation



Mission Vignette

Imagine that...

- An all-source analyst found suspiciously timed cyber-attacks on an allied NATO military base aligned with economic failures and coordinated protests.
- Using AI tools, she managed and cross-referenced classified and open-source data by storing, moving, and linking information in the IC's **optimized Cloud Environment**.
- With bolstered **compute, storage, and transport** capabilities, AI tools helped integrate agency-exclusive information with inter-agency intelligence for a fuller picture.
- Analysis revealed a coordinated effort to destabilize a NATO ally and recommends forward-deploying extra computing assets to **empower edge computing** if conflict breaks out.



The IC must continue to invest in its digital foundation, providing capabilities and data to all mission users, wherever they are, whenever they need it. The IC needs to be able to provide these capabilities seamlessly in multiple mission scenarios and support transformative initiatives such as data-centricity, and the expansion of AI services. Focus Area 1.0 calls for modernizing essential enterprise services and capabilities that enable broad mission outcomes today, and that are the foundation of advanced capabilities that will accelerate mission tomorrow.

Several challenges will need to be met in order to achieve this outcome. First, the IC must continue evolving from a single cloud provider, to an environment with multiple cloud providers and multiple cloud services. Paramount to this evolution is tailoring cloud capabilities to meet various mission needs. This journey is complex, ground-breaking, and nascent. Second, the IC must increase its compute, storage, and transport capacity, and prepare, now, to ensure the IC mission can operate at the tactical edge—including in disconnected, denied, intermittent, and/or with limited bandwidth (DDIL) environments, in order for the United States to maintain decision advantage over adversaries. Third, the IC must shore-up the networks on which the mission depends.

Key Initiatives (KI)

1.1 Make More World-Class Capabilities Available to Mission by Optimizing the IC's Cloud Environment

Whether it is a mission analyst producing finished intelligence, a human capital team onboarding new technologists, or acquisition and contracts officers procuring future capabilities, they all depend on cloud-based services and data for their success. The IC's cloud environment comprises enterprise capabilities as well as IC element hybrid and on-premise solutions. The Commercial Cloud Enterprise (C2E) contract provides IC elements with access to multiple industry-leading cloud service providers (CSP) to complement their hybrid and on-premise storage, compute, and other cloud-based services.

Each of the C2E CSPs offers unique “best of breed” capabilities. Enabling IC elements to optimize the respective strengths and unique capabilities available through a properly architected, multiple cloud infrastructure is essential. But these vendors are competitors, not teaming partners. Thus, doing this in a way that fosters the enhanced collaboration (Focus Area 3.0) and prepares for an AI-enabled future (Focus Area 5.0) will require that the IC rationalize the approach to an optimized multiple cloud environment. An evolution to multiple cloud will provide IC elements the right cloud for the right problem and still get needed data to anyone, anywhere, anytime, under any conditions, in accordance with appropriate authorizations and need-to-know.

The cloud evolution is a delicate balancing act that will present technical, operational, and acquisition challenges as time goes on, that, if not addressed, may have significant mission and cost implications. In the near-term, it will be important to provide tools to support IC elements choosing the right capability, service, or computing solution for a given mission area as the IC works to optimize its multiple cloud environment.

Target Milestones:

- Fiscal Year (FY) 25: Develop a tool, methodology, or process to help IC elements determine which approach and service provider would be most appropriate to meet their individual requirements.
- FY26: Provide enterprise guidance to ensure applications in one cloud can access and use data or applications in another cloud.

- FY27: Implement an IC-endorsed plan to rationalize the IC's multiple cloud approach, to include influencing service providers to strive for parity of their respective cloud offerings within and across all fabrics.

1.2 Meet the Demands of Tomorrow by Advancing and Scaling Compute, Storage, and Transport

The demand for compute, storage, and transport capabilities will continue to grow exponentially as AI expands across the enterprise to support mission and business systems. Advancements in these capabilities are continuously emerging that may optimally support the scope and scale of the IC's needs (to include AI, mission and business functions, and support for DDIL operations at the tactical edge). Additionally, the IC should continue prioritizing the resilience, scalability, and high availability of IC networks and transport services. Continued investment in networks enables transformative initiatives such as implementing a data-centric architecture (KI 4.2) and advancing AI at scale (KI 5.1).

Target Milestones:

- FY26: Increase scalability and capacity of IC high-performance compute capabilities to support enterprise and mission needs.
- FY27: Implement optimal compute and storage technologies that meet mission and enterprise needs.
- FY28: Optimize cloud services and enhance the efficiency with which IC users and mission partners access network-connected resources by increasing the coverage and capacity of the IC Network.
- FY29: Reinforce and engineer the IC network infrastructure and routing for maximum resiliency and integrity.

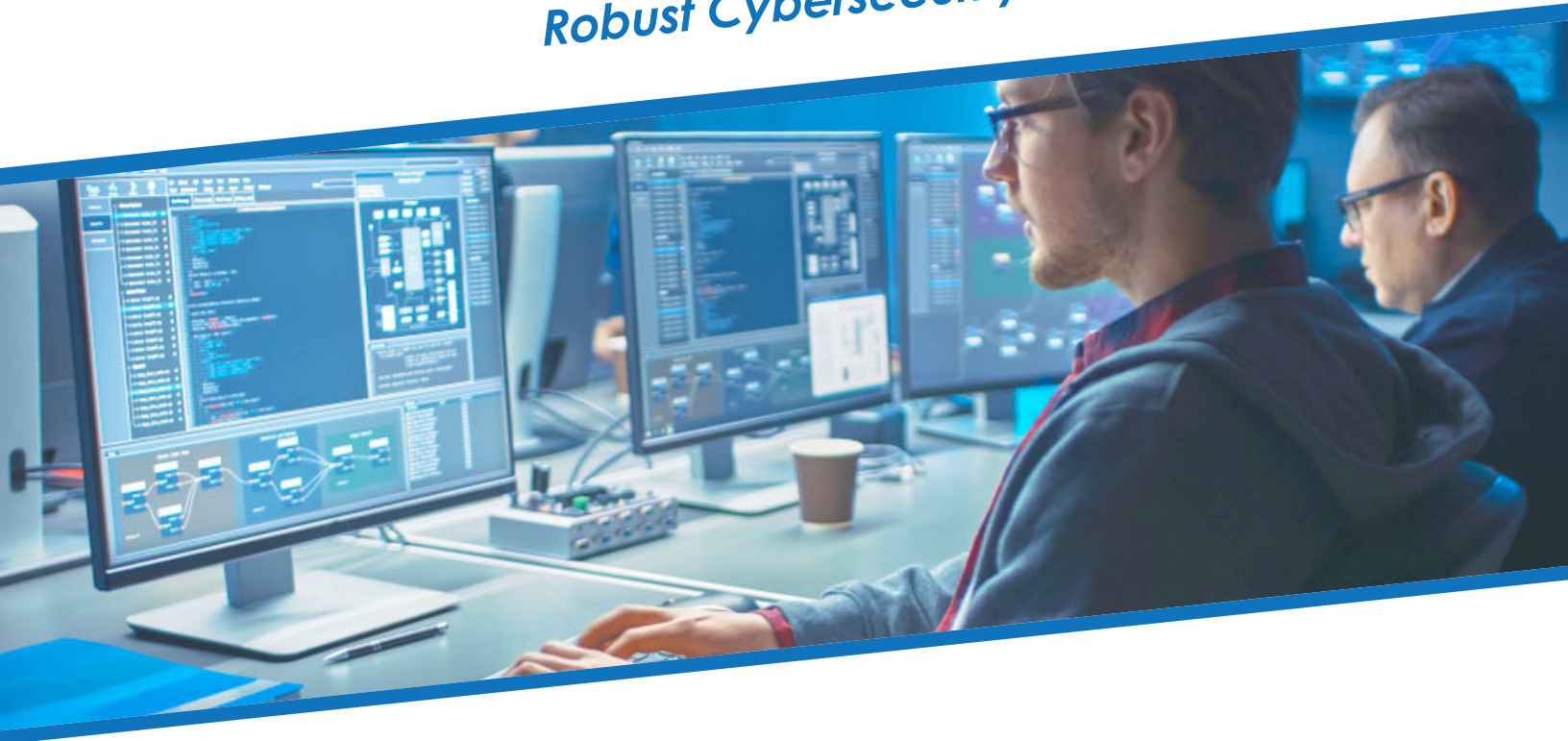
1.3 Enable the Intelligence Mission Anywhere by Empowering the Edge

Field operators need robust, secure, and mobile capabilities wherever they are (e.g., at the "edge"), including when disconnected from headquarters. From a technology perspective, this is a significant shift away from a headquarter-based orientation and towards one where edge locations have capabilities to operate independently or locally when necessary. This entails ensuring there is sufficient bandwidth, compute, and storage, as well as enabling DDIL environments.

Target Milestones:

- FY28: Develop and deploy necessary infrastructure (e.g., regional edge nodes) that enables mission success at the edge.
- FY30: Develop and implement secure mobility guidance (e.g., tools, methodologies, or a process) to permit edge-enabling capabilities to relocate on-demand, supporting dynamic mission needs (e.g., a new regional crisis).


Assure the Mission with Robust Cybersecurity



Mission Vignette

Imagine that...

- Two rival powers collaborated in deploying advanced AI for cyberattacks against the United States, a diversion tactic masking their imminent military advances on a NATO ally.
- A cyber defense team relied on **ZT architectures** that were protected from intrusions by **Quantum-Resistant Encryption**. These services blocked unauthorized access attempts to IC and DoD systems.
- Teams **used Mature and Integrated Security Coordination** by flexing to 24/7 operations and worldwide response across networks via **Secure/Hardened Cross Domain Security** systems.
- Because of the ubiquitous data access enabled by ZT, AI-enabled response systems outmaneuvered attackers and helped **Increase the Security and Speed of Software Delivery** to build updates that were quickly approved using a **modernized Enterprise Risk Management process**, systematically restoring compromised systems.



Cybersecurity continues to rise in visibility, investment, and strategic importance as the IC aggressively works to reinforce the protective blanket over the United States and its allies. The IC's technical leaders operate according to several crucial assumptions that drive the inclusion of cybersecurity as a Focus Area, which include, but go beyond, the IC's commitment to the *Intelligence Community Zero Trust Strategy 2023–2028*. Those assumptions include:

- **Adversaries will continue cyber operations:** Adversaries will also incorporate technological advancements. The shift towards unclassified remote work by IC element officers, and software development on the low-side, will present new opportunities for adversaries to infiltrate and exploit, which dramatically increases the complexity of threat assessment and detection. Adversaries' cyber operations will demand quick and coordinated response by the IC to limit damage.
- **Cybersecurity and mission are inseparable:** Mission success now depends intrinsically on strong and resilient IT and cybersecurity.
- **A transformation is underway in cybersecurity:** Cyber warfare changes traditional power dynamics, affording powerful asymmetric advantage to weaker actors. Previous cybersecurity approaches focused on protective barriers to keep adversaries from infiltrating infrastructure. The IC needs a new data-centric cybersecurity paradigm to protect data at the source, regardless of where and how it is accessed such that any breach effectively becomes a non-event.

Looking into the future, several things are clear. ZT principles are at the center of cybersecurity, and maturing ZT across the IC enterprise must remain a priority. ZT supports the transition of sensitive data siloes to data-centric enclaves (KI 4.3). Preparing for the future threat landscape requires the IC to continue the forward momentum to strengthen capabilities for integrated security coordination, from real-time threat detection and interagency alerting, to incident response and recovery, and ensuring privacy considerations are maintained. As quantum computing technology progresses, the potential to disrupt current encryption methods grows, making the adoption of quantum resistant cryptography solutions imperative. An IC-wide press to harden cross domain solutions that enable secure data transfer and systems, within and across security fabrics, will need renewed vigor.


A critical aspect of the IC's security fabric is mitigating risks while decreasing the time-to-market of software development and delivery. Innovating secure software development at mission speed requires common DevSecOps standards, tools, and approaches. This will expedite software through development and testing—per accepted authorization and accreditation processes—so IC elements can more quickly deploy the software on their own networks. Finally, as it moves towards infrastructure that enables data-centricity, the IC will need to modernize security enclaves to support the ability of analysts to have maximum authorized access to available data for mission within access control and need-to-know parameters.

The IC intends to do this through the following Key Initiatives in order to realize the benefits while mitigating the risks of the technological transformation underway.

Key Initiatives

2.1 Protect Our Mission from the Inside Out by Achieving ZT

The IC is committed to achieving the IC ZT strategic goals in the *Intelligence Community Zero Trust Strategy 2023–2028* within the published target timelines. Funding IC elements to achieve the goals and objectives for planning, designing, and embracing ZT capabilities across IC systems will significantly improve the



IC's defensive security posture, enable data sharing across security enclaves, and contribute to achieving interoperability among IC elements (KI 3.4). The Target Milestones below reflect these commitments by shifting the emphasis from a goal of achieving ZT to the deliberate achievement of ZT maturity. (Note: these dates are specific because they represent commitments from the *Intelligence Community Zero Trust Strategy 2023–2028*).

Target Milestones:

- 30 September 2025: Achieve “Basic” ZT Maturity.
- 30 September 2027: Achieve “Intermediate” ZT Maturity.
- FY28: Enforce ZT maturity within IC enclaves.
- 30 September 2029 (Tentative): Begin piloting services towards achieving “Advanced” ZT Maturity.

2.2 Deliver the Right IT at the Right Time through Modernized Enterprise Risk Management

IC Enterprise Risk Management must modernize, with an emphasis on evolving the Authority to Operate (ATO) process. Continuous Authority to Operate (cATO) is a proactive approach that treats IT security as a sustained commitment, promoting regular system maintenance and updates. cATO shifts away from viewing ATO as a one-time achievement. Instead, IC elements would implement cATO processes based on continuous monitoring and risk-scoring in accordance with the agreed-upon Risk Management Framework (RMF). This will empower Authorizing Officials (AO) throughout the IC while promoting collective efforts toward maintaining robust and up-to-date IT systems in line with the letter and spirit of Intelligence Community Directive (ICD) 503. Evolving the ATO process means IC elements need to trust each other's bodies of evidence that grant ATO. They need to be able to trust not only the software, but all of the physical locations where it is being managed.


The IC's move to a multiple cloud environment (KI 1.1) presents the IC with an opportunity to evolve the ATO process and introduce more automation into the RMF and decision support process, while keeping humans fully in charge of the ultimate decision-making. The development community needs updated baseline standards and security minimums to increase security and speed of software delivery (KI 2.4).

Target Milestones:

- FY24: Establish IC standards, tools, and best practices that streamline delivery of IT with the RMF Authorization Process.
- FY27: Update the ATO and RMF Authorization Processes to account for streamlining delivery of cloud services and technologies and to address any applicable facility countermeasures that may exist under certain conditions (e.g., radio frequency (RF) emanation).
- FY30: Automate continuous authorization recommendations of IC systems to inform authorization decisions.

2.3 Strengthen the IC's Collective Defenses by Maturing and Integrating Security Coordination

Improving cybersecurity involves moving towards automated integration of threat detection and alerting with security risk management data. Integrating endpoint security events, cyber threat intelligence, vulnerability scans, risk assessment, and authorization data with filtered results (agreed upon by the elements) into an interagency capability to measure the overall risk or threat posture of the IC IE will improve timeliness and accuracy of security situational awareness for IC elements.



Leveraging real-time, automated alerts minimizes human error and drastically reduces response times, making systems more robust against advanced cyberthreats. The IC Security Coordination Center (IC SCC) is the IC's Federal Cyber Center. The IC SCC collects and distributes indicators of suspicious or malicious activity across all IC element Security Operations Centers, which allows a new perspective for effectively spotting patterns and anomalies.

Target Milestones:

- FY27: Institute standards and common language policies to support real-time threat detection and alerting.
- FY28: Deploy IC-wide integrated threat detection and real-time interagency alerting.

2.4 Increase Security and Speed of Software Delivery through DevSecOps

Matching the pace of innovation while not compromising security is important as the IC becomes an AI-enabled enterprise in the next five years. Maturing how the IC designs, develops, secures, and operationalizes software (e.g., DevSecOps) is essential to increasing the security and speed of software delivery.

This KI encourages IC elements to adopt common DevSecOps standards, tools, playbooks, best practices, and processes for greater cohesion among elements. Using a “build low, push high” software approach with secure practices, the IC aims to increase workforce flexibility, speed up development, and align software versions across security domains.

The IC made significant advancements over the last decade to publish IC-endorsed best practices and develop and mature customizable DevSecOps environments that can be used by other IC elements that may not be able to develop their own. Moving towards a future where IC elements consistently employ best practices and have access to approved enterprise DevSecOps platforms that they either own or consume from others is essential to achieve this initiative.

Finally, gaining trust in vendors’ design, build, and delivery processes are key to strengthening the security of the IC software supply chain. Although individual IC elements’ insights into their software suppliers’ security parameters is beneficial, establishing an IC end-to-end framework is necessary for a consistent level of security and trust in IC interlocutors. To accomplish this, there should be approved standards for Software Bill of Materials, improved code and component signing infrastructure, and continued hardening of the software build and distribution infrastructure.

Target Milestones:

- FY25: Self-certify compliance with the IC’s published DevSecOps best practices and software assurance practices.
- FY26: Develop IC-endorsed guidance (e.g., establishing an end-to-end framework, approved standards for Software Bill of Materials) and approval process for enterprise DevSecOps platforms.
- FY30: Use an approved enterprise DevSecOps platform (that IC elements own or consume) in accordance with the IC-endorsed guidance.

2.5 Keep Our Most Sensitive Intelligence Safe by Realizing Quantum Resistant (QR) Cryptography

Cryptographic security in a post-quantum world will be pivotal for safeguarding data and digital communications. This includes the development and deployment of advanced cryptographic algorithms designed to be secure against threats from quantum computers, both in commercially available and government devices. Deploying advanced cryptographic algorithms, designed to be secure against threats from quantum computers, ensures the continued confidentiality of critical data and safeguards against future foreign capabilities at enterprise scale.

Target Milestones:

- FY27: Develop and deploy QR cryptography solutions to bolster the confidentiality of IC networks and transport services.
- FY29: Develop and deploy QR cryptography solutions within IC services (e.g., Identity, Credential, and Access Management to ensure non-repudiation of IC operations).

2.6 Batten Down the Hatches by Securing/Hardening Cross Domain Solutions (CDS)

Modern CDS will assist the IC in staying ahead of threats, enabling mission analysts to access and transmit data securely across security domains at headquarters and edge locations. The IC also needs the ability to develop and acquire leading-edge software capabilities and nimbly use them in accordance with authorizations across security domains. Thus, software developers require the ability to move software and related code between domains (e.g., from the unclassified to top secret fabrics). CDS makes this mission capability possible by helping to mitigate controlled boundary risks.

It will be critical that the IC work together to eliminate controlled boundary risk and this starts with knowing what those boundary risks are and knowing about the CDS. IC elements will continue to need the flexibility to develop bespoke tactical CDS that are responsive to unique mission needs. Outside of that, ensuring only acknowledged and designated CDS service providers operate CDS components within the IC can help eliminate these risks. The IC will establish governance for cloud-based and contractor-managed CDSs to ensure consistent security in all provided services, and other actions required by Raise-the-Bar (RTB), in accordance with National Security Memorandum 8 (NSM-8).

Target Milestones:

- FY26: Provide or update enterprise guidance and standards (including RTB) to promote the transition to secure and designated CDSs.
- FY28: Designate and deliver CDSs in accordance with IC standards and best practices.
- FY30: Require and ensure that CDS customers only use officially designated CDS (and provide a waiver process).


Enable the Mission with Modern Practices and Partnerships



Mission Vignette

Imagine that...

- The all-source team examined data, forecasted resource deficits, and interpreted both allied and adversary media, delivering a holistic assessment of the threat that indicated an imminent ground invasion.
- The analysis team grew, fostering **Agile and Non-Traditional Partnerships** with NATO analysts and boots-on-the-ground allied troops.
- AI-enabled translation tools **Enhanced and Extended Collaboration** across languages and network fabrics, making communication as seamless as possible and **Achieving Ubiquitous IT Accessibility** of data for those authorized to see it.
- The **Advanced Interoperability Among IC Elements** with shared services accelerated synthesized cross-fabric, cross-agency, cross-partner intelligence using shared AI models and shared AI-derived results.
- Their assessment highlighted numerous response options and focused on counter-messaging to thwart the destabilizing efforts and rebuild regional stability.



The IC is a complex federation requiring a profound and unified effort to achieve mission success on all fronts. The IC's ability to harness the collective contributions of the IC elements (as well as those of our partners) is a significant discriminator in determining mission success in the ever-evolving threat landscape. This necessitates a delicate balance of empowering IC elements to carry out their individual missions within the confines of their authorities, while enabling joint missions, information sharing, and collaboration to function seamlessly and dynamically.

Enabling the mission includes removing the barriers and obstacles that stand in the way of dynamic collaboration and information sharing. Embracing modern and leading-edge advancements in IT to overcome traditional challenges and put advantages at the fingertips of the end-user is essential. The limits of collaboration and information sharing are far beyond the internal IC and the Top Secret/Sensitive Compartmented Information (TS/SCI) fabric. It includes “catching up” the other fabrics with robust capabilities and standards.

Furthermore, it includes strengthening our key partnerships and cultivating ad-hoc, dynamic, and non-traditional partnerships to ensure mission success in the face of a dynamic threat landscape. At the user level, designing for an optimal user experience and ubiquitous IT accessibility is key for tapping into the full potential of the IC's workforce. At the enterprise level, continuing to advance interoperability between IC elements through deliberate guidance and IT delivery enables operational efficiency at scale.

Underpinning this Focus Area is an agile, adaptive, and coordinated governance fabric that fosters enterprise orchestration and cooperative decision-making.

Key Initiatives

3.1 Connect Our People by Enhancing and Extending Collaboration

Shoring-up gaps that impede ubiquitous collaboration is critical for mission success and enabling the infusion of more modern approaches to connect the right people, at the right time, and in the right way. This includes extending capabilities to other fabrics (beginning with the unclassified fabric).

The introduction of immersive and virtual technologies can transform collaboration and even tradecraft, by bringing people together in virtual realms that transcend traditional barriers such as geographic dispersion. The use of common virtual play-spaces provides a risk-free setting to practice complex operations, create virtual training scenarios, test strategies using virtual reality training equipment, or lower risks associated with gathering important intelligence data in the real-world.

Target Milestones:

- FY25: Extend IC guidance (e.g., collaboration reference architecture) to account for all fabrics (starting with the unclassified fabric) to guide the delivery of required collaboration capabilities and standards to satisfy enterprise needs.
- FY27: Modernize collaboration services and deliver federated solutions that fulfill capability gaps to enable ubiquitous collaboration across all fabrics.
- FY30: Incorporate virtual and immersive technologies and environments into the IC to support robust collaboration, training, and tradecraft.

3.2 Enable Dynamic Information Sharing by Cultivating Agile and Non-Traditional Partnerships

Mission success against threats depends on strong partnerships. To address new and emerging threats, the IC needs to accelerate and expand the use of ready-made partnership solutions. This “out-of-the-box” partnership approach enables the IC to constitute and dissolve ad-hoc, non-traditional IC partnerships in an agile way to include the full array of private sector and other important mission partners. Five Eyes Enterprise (5EE) and third-party (3P) partnerships need to be bolstered and fortified to support persistent and ad-hoc mission needs.

Target Milestones:

- FY25: Develop and deliver joint guidance, standards and solutions that enable increased collaboration and information sharing with partners (e.g., IC, DoD, FSLTT governments, private sector entities).
- FY26: Support or extend the services provided to the 5EE to enable evolving intelligence needs.
- FY27: Enable ad-hoc and persistent collaboration and mission analysis in a common and plug-and-play virtual environment with third party partners.

3.3 Tap into the Full Power of the IC Talent Pool by Achieving Ubiquitous IT Accessibility

The IC needs to be able to tap into the entire talent pool by realizing IT accessibility at scale and improving the user experience for all users. User-facing IT assets should be perceivable, operable, understandable, and robust for all members of the IC workforce.

Target Milestones:

- FY27: Deliver common IT tools (e.g., closed captioning), shared services, peripherals and platforms to support ubiquitous IT accessibility across the enterprise and to enhance the user experience.

3.4 Put the Multi-INT in Intelligence by Advancing Interoperability Among IC Elements

The intelligence mission continues to move towards a multi-element, multi-INT paradigm, bringing the best of breed from different elements and specific INTs to solve mission problems. As a complex federation of elements, missions, and authorities, the IC needs to foster integration at the “seams” of IC elements so they can interoperate by default and enable multi-element, multi-INT outcomes by default. These seams involve IT (e.g., networks, applications), policies, and standards. Continuing to advance IT, policies, and standards that foster interoperability among the IC elements will increase operational efficiencies and mission success.

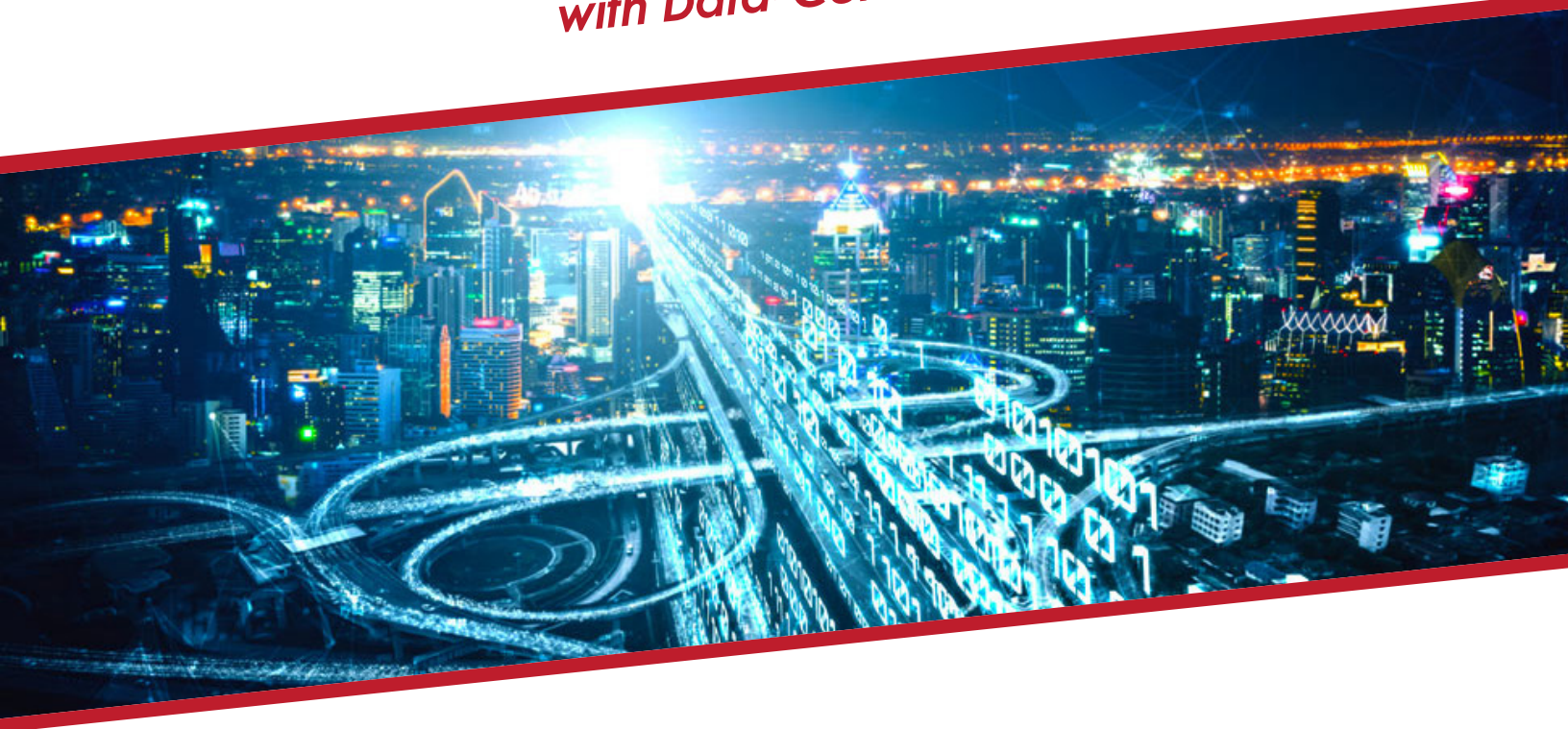
The IC is a multi-fabric enterprise, operating missions and enterprise functions (e.g., DevSecOps, AI model sharing) on TS/SCI, Secret, Controlled Unclassified Information, and Unclassified fabrics and within each, more discrete network and security domains. The IC needs to promote and introduce more modern and effective multi-fabric capabilities and standards to support enterprise functions and mission objectives. Doing so will also support DevSecOps improvements (KI 2.4), AI model development and training (KI 5.1), and multi-fabric intelligence operations.

Target Milestones:

- FY26: Deliver guidance, standards, and services for enabling interoperability among IC elements at specific layers of the IC IT architecture (e.g., networks, data services, compute/storage platforms, workflows, etc.).
- FY28: Deliver enterprise guidance and standards to promote multi-fabric capabilities and standards to support mission and enterprise needs.

Focus Area 4.0


Enhance the Mission with Data-Centricity



Mission Vignette

Imagine that...

- The all-source and cyber teams collaborated with NATO special forces to decrypt enemy communications, including radio, encrypted messages, and captured cell phone data.
- As information was captured locally, **Realizing End-to-End Data Management** by automatically sending the most important data back to U.S. **Data-Centric Enclaves** when secure bandwidth was available.
- Processes and standards enabled data as a product to be consumed by many analytic tools across classification levels and with NATO allies.
- The team extensively analyzed the voices and speech patterns of enemy commanders from captured phone and communications intercepts to make the data mission ready by storing these in reusable forms for future exploitation that were AI-ready for future mission support.



The intelligence mission is inherently one of data, whether is it collected, acquired, analyzed, or generated. The IC is an ecosystem of data organizations that collect, acquire, and analyze information for knowledge to derive and provide intelligence insights from the warfighter to the senior policymaker. For technologists, data-centricity involves treating data as a fixed, valuable asset that does not change regardless of the application or technology used to access it. Data-centricity is also a mindset that acknowledges the need and opportunity to present data as a product for reuse, enabling decision-making, operations, and innovations to occur at mission speed.

Today, too much of the IC's data is stove-piped and not accessible, interoperable, or reusable across an individual organization, the IC, or with partners. It is often locked in secure networks and systems, taking on the classification of those systems and keeping intelligence-sharing a cumbersome challenge. The volume of intelligence data, however, is growing exponentially, from terabytes to zettabytes. In addition, IC data is not systemically tagged, cataloged, and conditioned, which limits the use of modern methods and new technologies. To maintain U.S. national security and ensure a global strategic decision advantage, the IC; FSLTT partners; defense coalition; commercial industry; and international partners need to collaboratively share and exploit data in near real-time, and in accordance with legal, privacy, civil liberties, and policy authorities.

The *IC Data Strategy 2023–2025*, accompanied by the purposeful adoption of an IC-endorsed Data-Centric Framework, will create operational advantages, drive advanced analytics, increase the speed of decision-making, promote knowledge management and sensemaking, and enable human-machine teaming outcomes. It will optimize the speed of intelligence exploitation and delivery through a distributed data ecosystem, and a linked network of knowledge artifacts, that promotes enterprise-level data interoperability and use of advanced analytics and AI. The time is now to deliver the infrastructure and enable data-centricity if the IC is to retain superiority in an increasingly hyper-connected, data-driven, AI-powered world.

Key Initiatives

4.1 Expedite Mission Outcomes by Realizing End-to-End Data Management

To achieve data-centricity at scale, IC elements must effectively govern and manage data more cohesively. This demands comprehensive, domain-appropriate, end-to-end data management for all new collection and data acquisitions, including mission, commercial, and business. Data management planning, at the enterprise level, would help align complex data lifecycle management activities and provide linkages to critical mission architectures (e.g., collection). Through deliberate guidance and commitment, these plans will increase the adoption of IC Data Services and applied advanced analytics and AI. Data management plans are crucial for effective governance of systems data, enabling integration with existing and lineage datasets, improving data conditioning, and ensuring data reliability and pedigree, data discoverability and accessibility, reliability, and usability at scale.

Target Milestones:

- FY26: Deliver guidance and tools that enable end-to-end data management, including the creation, execution, reporting, managing, and automation of data management plans across the IC.



4.2 Maximize Intelligence Value by Implementing a Data-Centric Architecture

To achieve data-centricity, IC data must be valued as a strategic product. Data-centricity requires deliberate guidance to establish and leverage common data standards, models, services, and enterprise digital policies for legal, compliance, and security frameworks. Promoting a distributed data-centric architecture, while overlaying IC standards and IC element standards, will complement a decentralized data ecosystem that integrates data collected across currently stove-piped intelligence organizational domains and disciplines. This will guide the simplifying of data exchanges through standard application programming interfaces and foster more advanced AI/Machine Learning (AI/ML) capabilities. The result is that IC systems will work together more seamlessly, and it will be easier to integrate new technologies—ultimately leading to better, faster, and more efficient collaboration that will expedite analytic outcomes and streamline data sharing among the IC, DoD, FSLTT, private sector entities, and international partners.

Target Milestones:

- FY26: Develop and deliver an IC Data Reference Architecture to promote data-centric principles, including outlining standards, methods, tools, and services to enable data-centricity at scale.
- FY27: Develop and deliver tools and services that IC elements and specific functions (e.g., business, cyber, and/or mission-specific functions) can leverage to support, and be part of, the IC's data-centric architecture.

4.3 Empower the Analyst by Transitioning Sensitive Data Siloes to Data-Centric Enclaves

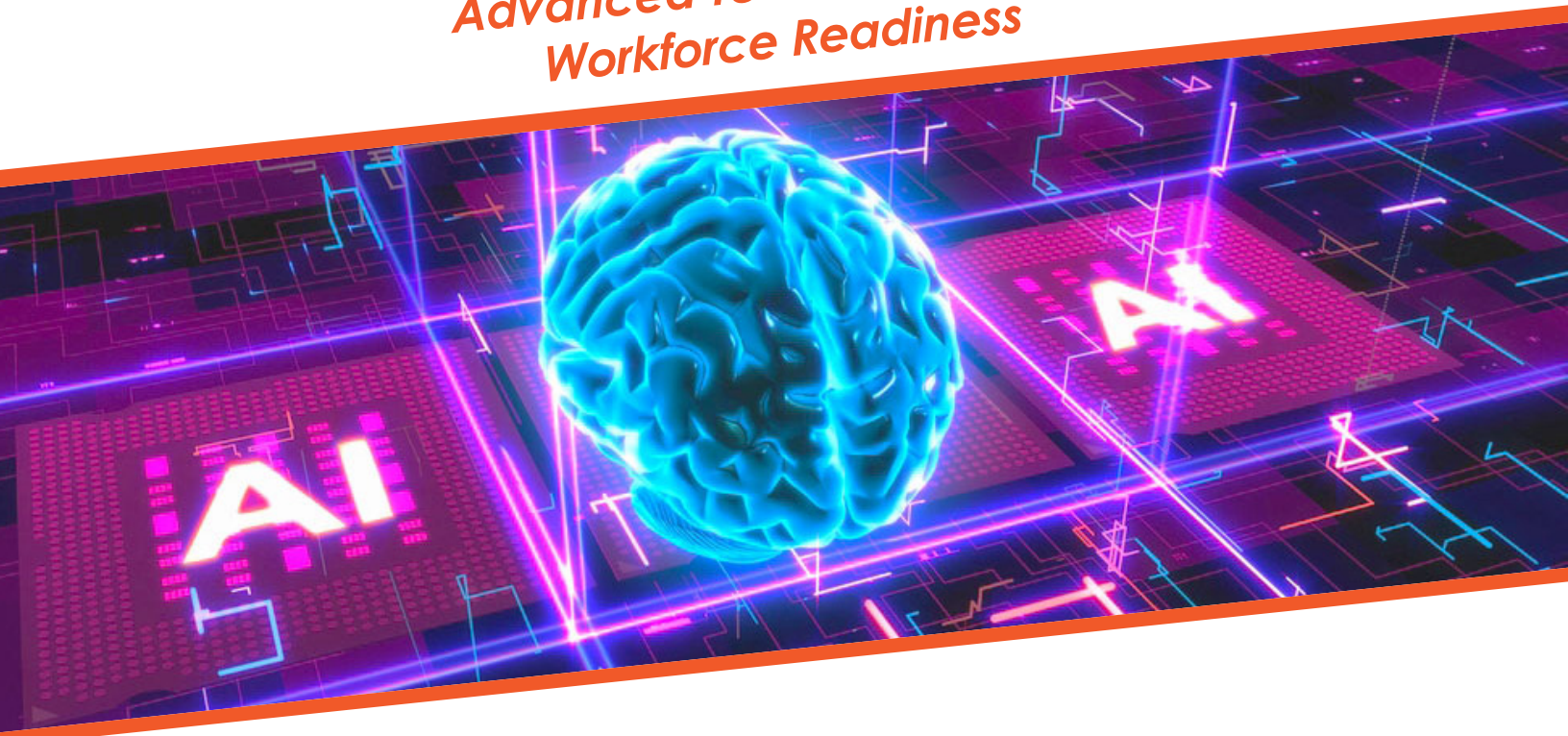
Sensitive data resides across the IC in dispersed enclaves, implemented and siloed to provide necessary specialized data protections within the requisite security fabrics and compartments. It is labor-intensive and time-consuming for IC analysts, with appropriate clearances and access authorizations, to discover and access available data across enclaves.

This initiative, which complements and relates closely to other data-centric initiatives, aims to break down traditional barriers to information discovery and use (e.g., network and application boundaries). IC users with appropriate clearances and access authorizations should be able to search and discover relevant available data, simultaneously, within and across multiple enclaves to more efficiently and effectively achieve the intelligence mission.

Target Milestones:

- FY26: Deliver guidance, standards, and services that prepare and condition data resources that reside within sensitive enclaves to be discovered and accessed by any IC user with the appropriate clearances and access authorization.


Accelerate the Mission with Advanced Technologies and Workforce Readiness



Mission Vignette

Imagine that...

- The adversary, avoiding full-scale war, persistently dispatched troops and tanks to disrupt and damage allied infrastructure under the pretext for liberating local cities from Western influence.
- Analysts at two agencies used **Advanced AI at scale** to triage mountains of data, teeing results up for other IC experts, and ensuring data accuracy.
- Their knowledge of the situation helped **Prime the Future Workforce**, providing training and guidance on using AI tools to fortify key infrastructure and insight into how their ally could defend and rebuild.
- They used AI systems to amplify global awareness, identify destroyed infrastructure, and guide other federal agencies and foreign partners in providing support, all from satellite imagery.
- Their work demonstrated the transformative power of technology in **Preparing for Over-the-Horizon Capabilities** by responding to this complex global crisis.
- Cross-agency sharing of data and AI models across data networks accelerated collaboration, insight generation, and mission support in unprecedented ways.



AI and other emerging capabilities represent urgent and tangible transformative opportunities that can accelerate the mission. The IC continues to increase investment in AI services and capabilities, as well as workforce talent that can deliver decision advantage and mission success over our adversaries. By leveraging AI, the IC will rapidly advance sensing capabilities, collections, advanced analytics, and knowledge integration.

To realize the promise of AI, the IC must deliver enterprise capabilities, set appropriate policy and guidance, and embrace the enabling technologies such as compute, storage, and transport (KI 1.2) underpinning responsible AI governance. This includes the application of mission-focused AI techniques, tools for ensuring accountability, and systems that embed ethical considerations within AI decision-making. The promise of AI depends on advancing the KIs in the other four Focus Areas.

Additionally, it is not too early to prepare for emerging computing paradigms that go beyond AI so that the IC is ready to leverage these when they become available.

The rapid pace of advancements in technologies and paradigms (to include AI) will continue to have a profound positive impact on the business of intelligence. Embracing these advancements requires a deliberate focus on ensuring the workforce is sufficiently trained and witting of them.

Key Initiatives

5.1 Unleash More, Better, Faster by Advancing AI at Scale

Today, the process of performing analysis and producing finished intelligence reports are time and labor intensive. By adopting AI services at scale, analysts can reduce the time it takes to perform some tasks from days or weeks, to minutes and seconds, saving time for more human-centric analytic activities. To get there, the IC needs to determine the key AI enabling capability gaps, deliver solutions that address them, and foster adoption of AI at scale.

Target Milestones:

- FY25: Develop enterprise guidance (e.g., AI architecture, standards, utilization policy) to support the delivery of AI enabling services and mature IC-wide utilization.
- FY26-30: Deliver AI enabling services at scale (e.g., Model Repository, Training Data).

5.2 Meet the Future When It Arrives by Preparing Now for Over-the-Horizon Capabilities

Looking even further into the future, emerging computing paradigms (such as probabilistic and quantum) and other leading-edge technologies will offer significant advantages over classical approaches. It is imperative that the IC conducts research in these and other technologies to be prepared to exploit them for mission applications and defend against their potential use by adversaries if and when they mature.

Target Milestones:

- FY26: Analyze what impacts quantum and other over-the-horizon technologies are expected to have on IC IT systems, and develop plans to adjust IC IT infrastructure to address these challenges.

5.3 Capitalize on Tomorrow's Capabilities by Priming the Future Workforce

The IC needs to improve and deepen the skillsets and proficiencies of the IT workforce to support advanced technologies and modern tradecraft.

Target Milestones:

- FY27: Identify critical skillsets for the future IT workforce (e.g., Artificial Intelligence, IT Accessibility, Quantum Computing) and develop policies and incentives (e.g., STEM-based incentives) to support recruiting and retaining people with these skillsets.



Appendix A

References

- Executive Order 14028, *Improving the Nation’s Cybersecurity*, May 2021
- Executive Order 14110, *The Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, October 2023
- National Security Memorandum 8 (NSM-8), *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, January 2022
- National Security Memorandum/NSM-10, *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, May 2022
- *The National Intelligence Strategy*, August 2023
- *The National Cybersecurity Strategy*, March 2023
- Intelligence Community Directive (ICD) 502, *Integrated Defense of the Intelligence Community Information Environment*, March 2011
- Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management*, July 2015
- The AIM Initiative, *A Strategy for Augmenting Intelligence Using Machines*, March 2018
- *The Intelligence Community Information Technology Enterprise Strategy 2022–2027*, December 2022
- *The IC Data Strategy 2023–2025*, June 2023
- *The Improving Cybersecurity for the Intelligence Community Information Environment Implementation Plan 2.0*, November 2022
- *The Intelligence Community Zero Trust Strategy 2023–2028*, May 2024
- NIST SP 800-218, *Secure Software Development Framework Version 1.1: Recommendations for Mitigating the Risks of Software Vulnerabilities*, February 2022
- *The Intelligence Community Data Management Lexicon*, January 2022

