National Intelligence Strategy

of the United States of America

2019

The National Intelligence Strategy
of the United States of America

IC Vision

A Nation made more secure by a fully integrated, agile, resilient, and innovative Intelligence Community that exemplifies America's values.

IC Mission

Provide timely, insightful, objective, and relevant intelligence and support to inform national security decisions and to protect our Nation and its interests.

This National Intelligence Strategy (NIS) provides the Intelligence Community (IC) with strategic direction from the Director of National Intelligence (DNI) for the next four years. It supports the national security priorities outlined in the *National Security Strategy* as well as other national strategies. In executing the NIS, all IC activities must be responsive to national security priorities and must comply with the Constitution, applicable laws and statutes, and Congressional oversight requirements.

All our activities will be conducted consistent with our guiding principles: We advance our national security, economic strength, and technological superiority by delivering distinctive, timely insights with clarity, objectivity, and independence; we achieve unparalleled access to protected information and exquisite understanding of our adversaries' intentions and capabilities; we maintain global awareness for strategic warning; and we leverage what others do well, adding unique value for the Nation.

From the Director of National Intelligence

As the Director of National Intelligence, I am fortunate to lead an Intelligence Community (IC) composed of the best and brightest professionals who have committed their careers and their lives to protecting our national security. The IC is a 24/7/365 organization, scanning the globe and delivering the most distinctive, timely insights with clarity, objectivity, and independence to advance our national security, economic strength, and technological superiority.

This, the fourth iteration of the National Intelligence Strategy (NIS), is our guide for the next four years to better serve the needs of our customers, to help them make informed decisions on national security issues, and to ultimately keep our Nation safe. The NIS is designed to advance our mission and align our objectives with national strategies, and it provides an opportunity to communicate national priority objectives to our workforce, partners, oversight, customers, and also to our fellow citizens.

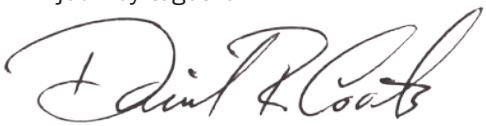
We face significant changes in the domestic and global environment; we must be ready to meet 21st century challenges and to recognize emerging threats and opportunities. To navigate today's turbulent and complex strategic environment, we must do things differently. This means we must:

- Increase integration and coordination of our intelligence activities to achieve best effect and value in executing our mission,
- Bolster innovation to constantly improve our work,
- Better leverage strong, unique, and valuable partnerships to support and enable national security outcomes, and
- Increase transparency while protecting national security information to enhance accountability and public trust.

This National Intelligence Strategy increases emphasis in these areas. It better integrates counterintelligence and security, better focuses the IC on addressing cyber threats, and sets clear direction on privacy, civil liberties and transparency.

We have crucial work before us. Our customers depend on us to help them to make wise national security decisions, and Americans count on us to help protect the Nation, all while protecting their privacy and civil liberties. We must provide the best intelligence possible to support these objectives; doing so is a collective responsibility of all of our dedicated IC professionals and, together with our partners, we can realize our vision.

Our ongoing goal is to continue to be the very best intelligence community in the world. Thank you for your service and for bringing your talent and commitment to the work of keeping our Nation safe each and every day. Thank you for your dedication to our mission and to the security of our fellow citizens as we take this journey together.



Daniel R. Coats
Director of National Intelligence

Strategic Environment

The strategic environment is changing rapidly, and the United States faces an increasingly complex and uncertain world in which threats are becoming ever more diverse and interconnected. While the IC remains focused on confronting a number of conventional challenges to U.S. national security posed by our adversaries, advances in technology are driving evolutionary and revolutionary change across multiple fronts. The IC will have to become more agile, innovative, and resilient to deal effectively with these threats and the ever more volatile world that shapes them. The increasingly complex, interconnected, and transnational nature of these threats also underscores the importance of continuing and advancing IC outreach and cooperation with international partners and allies.

Traditional adversaries will continue attempts to gain and assert influence, taking advantage of changing conditions in the international environment—including the weakening of the post-WWII international order and dominance of Western democratic ideals, increasingly isolationist tendencies in the West, and shifts in the global economy. These adversaries pose challenges within traditional, non-traditional, hybrid, and asymmetric military, economic, and political spheres. Russian efforts to increase its influence and authority are likely to continue and may conflict with U.S. goals and priorities in multiple regions. Chinese military modernization and continued pursuit of economic and territorial predominance in the Pacific region and beyond remain a concern, though opportunities exist to work with Beijing on issues of mutual concern, such as North Korean aggression and continued pursuit of nuclear and ballistic missile technology. Despite its 2015 commitment to a peaceful nuclear program, Iran's pursuit of more advanced missile and military capabilities and continued support for terrorist groups, militants, and other U.S. opponents will continue to threaten U.S. interests. Multiple adversaries continue to pursue capabilities to inflict potentially catastrophic damage to U.S. interests through the acquisition and use of weapons of mass destruction (WMD), which includes biological, chemical, and nuclear weapons.

In addition to these familiar threats, our adversaries are increasingly leveraging rapid advances in technology to pose new and **evolving threats**—particularly in the realm of space, cyberspace, computing, and other emerging, disruptive technologies. Technological advances will enable a wider range of actors to acquire sophisticated capabilities that were previously available only to well-resourced states.

No longer a solely U.S. domain, the democratization of **space** poses significant challenges for the United States and the IC. Adversaries are increasing their presence in this domain with plans to reach or exceed parity in some areas. For example, Russia and China will continue to pursue a full range of anti-satellite weapons as a means to reduce U.S. military effectiveness and overall security. Increasing commercialization of space now provides capabilities that were once limited to global powers to anyone that can afford to buy them. Many aspects of modern society—to include our ability to conduct military operations—rely on our access to and equipment in space.

Cyber threats are already challenging public confidence in our global institutions, governance, and norms, while imposing numerous economic costs domestically and globally. As the cyber capabilities of

our adversaries grow, they will pose increasing threats to U.S. security, including critical infrastructure, public health and safety, economic prosperity, and stability.

Emerging technologies, such as artificial intelligence, automation, and high performance computing are advancing computational capabilities that can be economically beneficial, however these advances also enable new and improved military and intelligence capabilities for our adversaries. Advances in nano- and bio-technologies have the potential to cure diseases and modify human performance, but without common ethical standards and shared interests to govern these developments, they have the potential to pose significant threats to U.S. interests and security. In addition, the development and spread of such technologies remain uneven, increasing the potential to drastically widen the divide between so-called "haves" and "have-nots."

Advances in communications and the democratization of other technologies have also generated an ability to create and share vast and exponentially growing amounts of information farther and faster than ever before. This **abundance of data** provides significant opportunities for the IC, including new avenues for collection and the potential for greater insight, but it also challenges the IC's ability to collect, process, evaluate, and analyze such enormous volumes of data quickly enough to provide relevant and useful insight to its customers.

These advances in communications and the democratization of other technologies have empowered non-state actors and will continue to exponentially expand the potential to influence people and events, both domestically and globally.

The ability of individuals and groups to have a larger impact than ever before—politically, militarily, economically, and ideologically—is undermining traditional institutions. This empowerment of groups and individuals is increasing the influence of ethnic, religious, and other sources of identity, changing the nature of conflict, and challenging the ability of traditional governments to satisfy the increasing demands of their populations, increasing the potential for greater instability. Some **violent extremist groups** will continue to take advantage of these sources and drivers of instability to hold territory, further insurgencies, plan external attacks, and inspire followers to launch attacks wherever they are around the world.

Increasing migration and urbanization of populations are also further straining the capacities of governments around the world and are likely to result in further fracturing of societies, potentially creating breeding grounds for radicalization. Pressure points include growing influxes of migrants, refugees, and internally displaced persons fleeing conflict zones; areas of intense economic or other resource scarcity; and areas threatened by climate changes, infectious disease outbreaks, or transnational criminal organizations.

All of these issues will continue to drive global change on an unprecedented scale and the IC must be able to warn of their strategic effects and adapt to meet the changing mission needs in this increasingly unstable environment. There will likely be demand for greater intelligence support to domestic security, driven in part by concerns over the threat of terrorism, the threat posed by transnational illicit drug and human trafficking networks, and the threat to U.S. critical infrastructure. Intelligence support to counter these threats must be conducted in accordance with IC authorities, with appropriate levels of transparency to the public, and with adequate protection for civil liberties and privacy.

00001001000110000001100101000111
00010000000100110001011101110101
00000110000101000001011101110101
00010001000100000001011101110101
100
80
60
40
20
00010010001010000010000000000001

Mission Objectives

The seven mission objectives broadly describe the activities and outcomes necessary for the IC to deliver timely, insightful, objective, and relevant intelligence and support to its customers. Mission objectives address a broad range of regional and functional topics facing the IC and their prioritization is communicated to the IC through the National Intelligence Priorities Framework.

The first three mission objectives address foundational missions of the IC which transcend individual threats, topics, or geographic regions. This is different from foundational military intelligence, which is intelligence on foreign military capabilities. As such, **foundational mission objectives** collectively represent the broadest and most fundamental of the IC's intelligence missions.

1 Strategic Intelligence

addresses issues of enduring national security interest.

2 Anticipatory Intelligence

addresses new and emerging trends, changing conditions, and underappreciated developments.

3 Current Operations Intelligence

supports planned and ongoing operations.

The next four mission objectives address specific, topical missions of the IC. The **topical mission objectives** are supported by the three foundational mission objectives and may contain elements of these. Other specific regional and functional issues, such as conflict areas and transnational criminal organizations, are implicitly covered by the mission objectives.

4 Cyber Threat Intelligence

addresses state and non-state actors engaged in malicious cyber activities.

5 Counterterrorism

addresses state and non-state actors engaged in terrorism and related activities.

6 Counterproliferation

addresses state and non-state actors engaged in the proliferation of weapons of mass destruction and their means of delivery.

7 Counterintelligence and Security

addresses threats from foreign intelligence entities and insiders.

National Intelligence and Intelligence Related to National Security means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(Executive Order 12333)

Strategic Intelligence

Identify and assess the capabilities, activities, and intentions of states and non-state entities to develop a deep understanding of the strategic environment, warn of future developments on issues of enduring interest, and support U.S. national security policy and strategy decisions.

Strategic intelligence is the process and product of developing the context, knowledge, and understanding of the strategic environment required to support U.S. national security policy and planning decisions. This work includes identifying and assessing the capabilities, activities, and intentions of states and non-state entities to identify risks to and opportunities for U.S. national security interests. Strategic intelligence involves assimilating a variety of information—including knowledge of political, diplomatic, economic, and security developments—to create a deep understanding of issues of enduring importance to the United States. Strategic intelligence also provides in-depth assessments of trends and developments to recognize and warn of changes related to these issues that will affect the future strategic environment.

The foundation for strategic intelligence requires developing and maintaining a deep understanding of the strategic environment, to include transnational issues such as terrorism and transnational organized crime, and the capabilities, activities, and intentions of states and non-state entities necessary to support U.S. national security policy and planning decisions. The IC must master strategic intelligence issues through research, knowledge development, collaboration with experts within the IC, and outreach to experts in academia and industry, as well as the use of advanced analytics and tradecraft to provide in-depth assessments and the strategic context for a wide variety of policy and strategy communities.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Develop and maintain capabilities to acquire and evaluate data to obtain a deep understanding of the global political, diplomatic, military, economic, security, and informational environment.**
- **Build and maintain expertise and knowledge of issues of enduring strategic importance to the United States, and assess trends and developments related to these issues to identify changes that would affect U.S. national security interests and to identify strategic risks and opportunities.**
- **Provide in-depth assessments, context, and expertise about the strategic environment, including the capabilities, activities, and intentions of key state and non-state entities, to inform U.S. national security policy and strategy development.**

Anticipatory Intelligence

2

Identify and assess new, emerging trends, changing conditions, and underappreciated developments to challenge long-standing assumptions, encourage new perspectives, identify new opportunities, and provide warning of threats to U.S. interests.

Anticipatory intelligence involves collecting and analyzing information to identify new, emerging trends, changing conditions, and undervalued developments, which challenge long-standing assumptions and encourage new perspectives, as well as identify new opportunities and warn of threats to U.S. interests. Anticipatory intelligence usually leverages a cross-disciplinary approach, and often utilizes specialized tradecraft to identify emerging issues from "weak signals," cope with high degrees of uncertainty, and consider alternative futures.

Anticipatory intelligence looks to the future as foresight (identifying emerging issues), forecasting (developing potential scenarios), or warning. Anticipatory intelligence explores the potential for cascading events or activities to reinforce, amplify, or accelerate conflict. It may uncover previously unconnected groups or regions and include indicators or benchmarks to identify key developments as trends change over time. Anticipatory intelligence assesses risk, intelligence gaps, and uncertainties by evaluating the probability of occurrence and potential effects of a given development on U.S. national security.

The complexity, scale, and pace of changes developing around the world test the IC's ability to deliver insightful and actionable intelligence with optimal fidelity, scope, and speed required to mitigate threats and exploit opportunities. The IC will expand its use of quantitative analytic methods while reinforcing qualitative methods, especially those that encourage new perspectives and challenge long-standing assumptions. With evolving intelligence requirements, anticipatory intelligence is critical for efficient IC resource allocation. The IC will improve its ability to foresee, forecast, and alert regarding potential issues of concern and provide the best possible opportunities for action to our national security customers.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Develop quantitative methods and data analysis techniques and tradecraft to improve the IC's ability to identify, analyze, and forecast changing conditions and emerging trends across multiple portfolios.**
- **Increase common understanding of the scope, definition, tradecraft, and methods of anticipatory intelligence across the community to develop workforce proficiency in these skills.**
- **Identify and work to remove the cultural, technological, human capital, and other barriers to incorporate anticipatory intelligence into the IC's routine analytic efforts.**
- **Produce and provide intelligence information and products that highlight emerging trends, changing conditions, and opportunities or threats in areas of limited customer focus to maximize decision advantage.**
- **Develop integrated capabilities to create alerts within the IC to provide timely and relevant warning to our customers, as well as to apprise them of opportunities.**

Current Operations Intelligence

3

Provide timely intelligence support to enable planned and ongoing operations.

Current operations intelligence is the collection, analysis, operations, and planning support that IC elements conduct to enable successful planned and ongoing operations. Current operations intelligence includes the intelligence necessary to support the time-sensitive needs of military, diplomatic, homeland security, and policy customers in times of conflict or crisis, but also provides opportunities to shape future operations and desired operational outcomes.

The IC will adapt to evolving operational requirements, maintain the robust support customers expect, and further enhance capabilities. Faced with a wide spectrum of operations in support of military, diplomatic, and homeland security activities, to include addressing transnational organized crime, the IC will prioritize its efforts and mitigate risk, operate in denied areas, balance forward presence with robust reach-back, and provide operational resiliency to more fully integrate intelligence with operations.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Provide timely intelligence support to enable planned and ongoing operations.**
- **Develop and maintain a robust, IC-wide intelligence architecture that delivers actionable, timely, and agile intelligence support to achieve and maintain operational decision advantage.**
- **Expand and enhance collaboration with domestic and global partners to maximize the effectiveness and reach of intelligence capabilities in support of operations.**
- **Conduct sensitive intelligence operations to support effective national security action.**

Cyber Threat Intelligence

4

Detect and understand cyber threats from state and non-state actors engaged in malicious cyber activity to inform and enable national security decisionmaking, cybersecurity, and the full range of response activities.

Cyber threat intelligence is the collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, targets, operational activities and indicators, and their impact or potential effects on U.S. national security interests. Cyber threat intelligence also includes information on cyber threat actor information systems, infrastructure, and data; and network characterization, or insight into the components, structures, use, and vulnerabilities of foreign cyber program information systems.

Despite growing awareness of cyber threats and improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years to come. Our adversaries are becoming more adept at using cyberspace capabilities to threaten our interests and advance their own strategic and economic objectives. Cyber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices. The IC must continue to grow its intelligence capabilities to meet these evolving cyber threats as a part of a comprehensive cyber posture positioning the Nation for strategic and tactical response.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Increase our awareness and understanding of adversaries' use of cyber operations—including leadership plans, intentions, capabilities, and operations—to inform decisions and enable action.**
- **Expand tailored production and appropriate dissemination and release of actionable cyber threat intelligence to support the defense of vital information networks and critical infrastructure.**
- **Expand our ability to enable diplomatic, information, military, economic, financial, intelligence, and law enforcement plans and operations to deter and counter malicious cyber actors and activities.**

Counterterrorism

Identify, understand, monitor, and disrupt state and non-state actors engaged in terrorism and related activities to defeat threats to the United States, our people, interests, and partners.

The dynamic nature of the terrorist threat facing the United States requires continued emphasis on intelligence collection and analysis. The IC is therefore an integral part of the national whole-of-government effort to protect our country from terrorist attacks. The IC works across agencies and with domestic and foreign partners to disrupt, dismantle, and defeat terrorists who threaten our homeland, our people, our interests, and our partners overseas.

The IC identifies and helps to eliminate terrorist safe havens and degrade the illicit financial networks that fund terrorist activities. The IC supports broader U.S. Government efforts to counter the spread of violent extremist ideology that drives terrorist actions and to leverage domestic and foreign partnerships and capabilities to strengthen our own capacity and resilience. The enduring and evolving nature of the threat, to include the threat of WMD terrorism, means that the IC must continue to pursue innovative approaches to collection and analysis to ensure counterterrorism (CT) efforts remain effective, efficient, and fully integrated.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Collect and analyze intelligence to enable the disruption of terrorist attacks and attack planning, as well as terrorism-related activities.**
- **Identify and warn of emerging and changing threats, trends, and violent extremist ideologies to develop opportunities to counter them.**
- **Broaden and deepen strategic knowledge of the global terrorism landscape to provide context to customers.**

Counterproliferation

6

Detect, characterize, and disrupt activities of state and non-state actors engaged in the proliferation of weapons of mass destruction (WMD) and their means of delivery to defeat WMD threats to the United States, our people, interests, and partners.

Proliferation is the development and spread of WMD, related technologies, materials, or expertise, and their means of delivery, including both indigenous development and transfers.

Counterproliferation discourages interest in WMD, denies or disrupts acquisition, degrades programs and capabilities, deters use, and mitigates consequences.

The IC must continue to implement a whole-of-government approach to advancing the enduring U.S. counterproliferation policy goals of discouraging interest in WMD, denying or disrupting acquisition, degrading programs and capabilities, including financial networks that fund proliferation activities, deterring use, and mitigating consequences. This issue is increasingly important as regional security dynamics evolve and as states, terrorists, and proliferators take advantage of rapidly emerging technological advances.

Many adversaries continue to pursue capabilities to inflict catastrophic damage to U.S. interests through the acquisition and use of WMD. Their possession of these capabilities can have major impacts on U.S. national security, overseas interests, allies, and the global order. The intelligence challenges to countering the proliferation of WMD and advanced conventional weapons are increasing as actors become more sophisticated, WMD-related information becomes broadly available, proliferation mechanisms increase, and as political instability erodes the security of WMD stockpiles.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Strengthen U.S. Government efforts to secure global WMD stockpiles, disrupt adversaries' programs, and prevent the transfer of WMD, related technologies, materials, or expertise.**
- **Bolster U.S. ability to anticipate and manage WMD crises, including potential disclosure, loss, theft, or use of WMD-related materials or weapons.**
- **Develop, maintain, and enhance intelligence capabilities to advance understanding of foreign WMD programs, related technologies, materials, or expertise to effectively inform interagency counterproliferation strategic planning and operations.**

Counterintelligence and Security

7

Detect, understand, deter, disrupt, and defend against threats from foreign intelligence entities and insiders to protect U.S. national and economic security.

Foreign Intelligence Entity (FIE) is any known or suspected foreign state or non-state organization or person that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

Insider Threat is the threat that an insider—any person with authorized access to any U.S. Government resource, to include personnel, facilities, information, equipment, networks, or systems—will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

The United States faces an increasingly complex and diverse set of counterintelligence (CI) and security challenges. Rapid technological advances are allowing a broad range of FIEs to field increasingly sophisticated capabilities and aggressively target the government, private sector partners, and academia. FIEs are proactive and use creative approaches—including the use of cyber tools, malicious insiders, espionage, and supply chain exploitation —to advance their interests and gain advantage over the United States. These activities intensify traditional FIE threats, place U.S. critical infrastructure at risk, erode U.S. competitive advantage, and weaken our global influence. To mitigate these threats, the IC must drive innovative CI and security solutions, further integrate CI and security disciplines into IC business practices, and effectively resource such efforts. While the authorities that govern CI and security and the programs they drive are distinct, their respective actions must be synchronized, coordinated, and integrated.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Drive integrated IC activities to anticipate and advance our understanding of evolving FIE threats and security vulnerabilities.**
- **Develop and implement new capabilities to detect, deter, and disrupt FIE activities and insider threats.**
- **Advance CI and security efforts to protect our people, technologies, information, infrastructure, and facilities from FIEs and insider threats.**
- **Strengthen the exchange of FIE threat and security vulnerability information among key partners and stakeholders to promote coordinated approaches to mitigation.**

FBI
POLICE

TECHNOLOGY
INTERNET
00001001000110000001100101000111
00010001001001010010000000000010
00000010000001110010000000000110
00001001000100100010000000000101
00010000000000010001100101000101
00010010000001000001100110000001

Enterprise Objectives

The seven enterprise objectives provide the foundation for integrated, effective, and efficient management of mission capabilities and business functions.

The first two enterprise objectives focus on general mission and business practices of the IC.

1 Integrated Mission Management

addresses IC mission capabilities, activities, and resources to achieve unity of effort.

2 Integrated Business Management

addresses IC business functions and practices to enable mission success.

The next five enterprise objectives focus on integration of IC efforts in specific areas for the successful completion of the mission objectives.

3 People

seeks to forge and retain a diverse, inclusive, and expert workforce.

4 Innovation

addresses the improvement of mission and business processes through new technologies, innovative thought, and advancements in tradecraft.

5 Information Sharing and Safeguarding

improves collaboration and integration while protecting information.

6 Partnerships

seeks to enhance intelligence through partnerships.

7 Privacy, Civil Liberties, and Transparency

seeks to protect U.S. values and enhance public trust.

Integrated Mission Management

Prioritize, coordinate, align, and de-conflict IC mission capabilities, activities, and resources to achieve unity of effort and the best effect in executing the IC's mission objectives.

Effective mission execution requires flexible, responsive, and resilient efforts to appropriately share knowledge, information, and capabilities across organizational boundaries; mission-focused centers have proven effective in achieving these ends. IC leaders will integrate, collaborate, and exchange feedback across priority areas to meet customer needs.

The IC must strike a balance between unity of effort and specialization, using the best of each to meet mission objectives. Integrated mission management drives collaboration, creates efficiencies, and minimizes redundancies, allowing the IC to effectively use available resources.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Provide leadership and community management to foster collaboration, streamline processes, and effectively manage resources to achieve IC mission objectives.**
- **Conduct integrated planning, analysis, collection, production, and dissemination to synchronize intelligence activities.**
- **Leverage IC capabilities and multi-disciplinary expertise to collaboratively anticipate intelligence problems, implement solutions, and enable innovation.**
- **Strengthen and integrate IC governance bodies to increase transparency, prioritize and optimize resources, balance tradeoffs, and manage risk.**
- **Drive integrated investment decisions and the delivery of multi-disciplinary, integrated capabilities to assure mission success.**

Integrated Business Management

2

Provide and optimize IC business functions and practices to enable mission success.

IC business functions and practices enable the community to perform its missions, activities, and operations. These functions and practices include the coordinated development, alignment, de-confliction, execution, and monitoring of strategies, policies, plans, and procedures needed to manage and secure the IC and its people, information technology, and physical infrastructure.

Effectively managing business functions and practices across the IC contributes to communication and collaboration, supports the efficient use of resources, enables resilience, and strengthens integration. Common standards, shared services, and best practices within IC authorities can increase efficiency, effectiveness, and accountability; successfully manage and mitigate risk; and improve business processes through data-driven reviews and performance measurements. The IC will promote and identify best business practices and functions to optimize solutions and increase collaboration to create a culture of continuous learning, innovation, and partnerships across the community. The IC must also develop flexible, risk-managed acquisition processes that deliver innovative capabilities, data, and expertise at mission pace.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Advance a dynamic approach to continuous evaluation and common security practices and standards to strengthen the security of the IC infrastructure.**
- **Pursue common strategies and best practices for acquisition and procurement across the IC to enhance the cost-effectiveness, efficiency, and agility of acquiring and procuring IC products and services.**
- **Implement IC-wide financial standards, processes, tools, and services to achieve fiscal efficiency, accountability, and security.**
- **Enhance strategy-based performance evaluation across the IC that leverages both government and industry best practices to enable informed IC business decisions and guide efficient application of resources.**
- **Explore innovative means to advance IC facilities, logistics, environmental, and energy programs to enable joint-use functionality; increase efficiency, sustainability, and supportability; and achieve total asset management.**
- **Manage risk to intelligence capabilities through IC-wide continuity efforts to foster resilience under all conditions.**

People

3

Forge and retain a diverse, inclusive, and expert workforce to address enduring and emerging requirements and enable mission success.

Diversity is a collection of individual attributes that together help IC elements pursue organizational objectives efficiently and effectively. These attributes include but are not limited to characteristics such as national origin, language, race, color, mental or physical disability, ethnicity, sex, age, religion, sexual orientation, gender identity or expression, socioeconomic status, veteran status, and family structure. **Inclusion** is a culture that connects each employee to the organization; encourages collaboration, flexibility, and fairness; and leverages diversity throughout the organization so that all individuals are able to participate and contribute to their full potential.

Linked together, diversity and inclusion drive innovation and enable the IC to attract and retain the highly-skilled workforce needed to meet mission requirements.

The IC is united in protecting and preserving national security, an objective that can only be met with the right, trusted, agile, and well-led workforce. IC personnel, including all civilians, military, and contractors, must adhere to the *Principles of Professional Ethics for the IC*. Effective approaches are needed to recruit, retain, develop, and motivate employees who possess skills that are fundamental to the intelligence mission, including critical thinking, foreign language, science, technology, engineering, and mathematics. The responsibility to lead and integrate the IC workforce extends beyond the IC's human capital, equal employment opportunity, and diversity and inclusion community to span the entire enterprise. Similarly, all IC employees are accountable for cultivating a performance-driven culture that encourages collaboration, flexibility, and fairness.

The IC must have effective tools and resources that integrate workforce planning, transformational leadership, continuous learning, information sharing, performance management, and accountability. Additionally, the IC will make long-term strategic investments in the workforce to promote agility and mobility throughout employees' careers, including joint duty rotations, and ensure that benefits, compensation, and work-life balance initiatives are fully considered and implemented wherever feasible.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Create an inclusive environment empowering managers and employees at all levels to take responsibility and ownership for the diversity of the organization.**
- **Take measures to proactively prevent discrimination, harassment, and fear of reprisal, enabling the workforce to perform at its highest potential.**
- **Shape a diverse workforce with the skills and capabilities needed to address enduring and emerging requirements.**
- **Invest in mid-level managers and leaders to ensure they are appropriately trained, supported, and held accountable.**
- **Pursue common business functions and practices for human capital, diversity and inclusion, and equal employment opportunity (EEO) compliance programs to enable informed IC human resource investments and decisions.**

Innovation

Find, create, and deploy scientific discoveries and new technologies, nurture innovative thought, advance tradecraft, and constantly improve mission and business processes to advance the IC in a rapidly changing landscape.

Innovation—through technological advancements and improved business practices—is critical to ensuring that the IC can provide the strategic and tactical decision advantage that policymakers and warfighters require. To continue meeting future challenges, the IC must drive new levels of innovation by proactively developing and rapidly incorporating breakthrough and incremental technologies, ideas, and constructs. The IC must also foster unconventional thinking and experimentation that address new, better ways of accomplishing the IC's mission, especially those approaches that emphasize acceleration, simplicity, and efficiency without sacrificing quality and outcomes. These approaches should increase insight, knowledge, and speed through artificial intelligence, automation, and augmentation, where applicable. To achieve this, IC leaders must be prepared to boldly accept calculated risks to attain high-value results, and accept the fact that initial failures may precede a successful outcome.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Conduct, leverage, protect, and operationalize groundbreaking research to create agile and revolutionary IC capabilities.**
- **Nurture an enterprise-wide atmosphere of innovation capable of rapidly and dynamically adapting to new challenges and opportunities.**
- **Explore novel operational applications of technology and other resources to advance tradecraft and achieve mission advantage.**
- **Continuously develop and adopt cutting-edge mission and business processes to improve intelligence capabilities and services.**

Information Sharing and Safeguarding

5

Develop, enhance, integrate, and leverage IC capabilities and activities to improve collaboration and the lawful discovery, access, retrieval, and safeguarding of information.

The IC **Information Environment (IE)** includes the individuals, organizations, and information technology (IT) capabilities that collect, process, or share Sensitive Compartmented Information, or that, regardless of classification, are managed by the IC.

Mission success depends on the right people getting the right information at the right time to inform decisionmaking. To do this, the IC will take a cutting-edge approach to appropriately access information, regardless of where the information resides. Information that is better organized into appropriate data formats and tagged with metadata to increase its quality and usability will aid the transition to information-centered intelligence processes. An integrated IC IE will enable the IC to protect against external and insider threats, maintain the public trust, protect privacy and civil liberties, and carry out its mission. To do this, the IC must continue to adopt modern data management practices to make IC data discoverable, accessible, and usable through secure, modernized systems and standards.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Identify, validate, prioritize, and address capability and policy requirements for the IC IE to enhance intelligence integration and operate as a secure, effective, and efficient IC enterprise.**
- **Increase the speed, portability, and trust of IC information system risk assessments to instill stakeholder confidence in the IC IE, and accelerate delivery of mission capability to users.**
- **Enhance foundational IC IT capabilities and infrastructure to increase mission effectiveness and reduce duplication.**
- **Develop and implement innovative means to manage, share, and protect intelligence information in accordance with law and policy.**
- **Leverage advanced analytics with modern data extraction, correlation, and enrichment capabilities to maximize the value of IC data.**

Partnerships

6

Optimize partnerships to enhance intelligence and better inform decisionmaking.

Partners consist of organizations and entities working with us to advance national security priorities, including the U.S. military, our allies, foreign intelligence and security services, other federal departments and agencies, as well as state, local, and tribal officials and private sector entities, as appropriate.

The IC's partnerships are fundamental to our national security. Effectively leveraging their collective capabilities, data, expertise, and insights make our partners force multipliers. The IC will optimize existing partnerships and forge new relationships to enhance intelligence and inform decisions.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Deepen mutual understanding and collaboration among partners to effectively inform decisions and enable action.**
- **Strengthen existing and develop new partnerships to increase access to information to meet mission needs, in accordance with applicable law.**
- **Institutionalize a strategic approach to partner engagement to facilitate collaboration and understanding.**

Privacy, Civil Liberties, and Transparency

7

Safeguard privacy and civil liberties and practice appropriate transparency to enhance accountability and public trust in all we do.

The Principles of Intelligence Transparency for the Intelligence Community provide general norms for the IC to follow in making information publicly available that enhances public understanding of intelligence activities while continuing to protect information when disclosure would harm national security.

The IC must be accountable to the American people in carrying out its national security mission in a way that upholds the country's values. The core principles of protecting privacy and civil liberties in our work and of providing appropriate transparency about our work, both internally and to the public, must be integrated into the IC's programs and activities. Doing so is necessary to earn and retain public trust in the IC, which directly impacts IC authorities, capabilities, and resources. Mission success depends on the IC's commitment to these core principles.

TO MEET THIS OBJECTIVE, THE IC WILL:

- **Incorporate privacy and civil liberties requirements into IC policy and programs to ensure that national values inform the intelligence mission.**
- **Engage proactively with oversight institutions and our partners to enhance public understanding and trust in the IC.**
- **Practice and promote appropriate transparency in the IC to make information publicly available without jeopardizing national security.**

PRINCIPLES OF INTELLIGENCE TRANSPARENCY FOR THE INTELLIGENCE COMMUNITY

The Principles of Intelligence Transparency for the Intelligence Community (IC) are intended to facilitate IC decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security. These Principles do not modify or supersede applicable laws, executive orders, and directives, including Executive Order 13526, Classified National Security Information. Instead, they articulate the general norms that elements of the IC should follow in implementing those authorities and requirements.

The Intelligence Community will:

1. Provide appropriate transparency to enhance public understanding about:
   a. the IC's mission and what the IC does to accomplish it (including its structure and effectiveness);
   b. the laws, directives, authorities, and policies that govern the IC's activities; and
   c. the compliance and oversight framework that ensures intelligence activities are conducted in accordance with applicable rules.

2. Be proactive and clear in making information publicly available through authorized channels, including taking affirmative steps to:
   a. provide timely transparency on matters of public interest;
   b. prepare information with sufficient clarity and context, so that it is readily understandable;
   c. make information accessible to the public through a range of communications channels, such as those enabled by new technology;
   d. engage with stakeholders to better explain information and to understand diverse perspectives; and
   e. in appropriate circumstances, describe why information cannot be made public.

3. In protecting information about intelligence sources, methods, and activities from unauthorized disclosure, ensure that IC professionals consistently and diligently execute their responsibilities to:
   a. classify only that information which, if disclosed without authorization, could be expected to cause identifiable or describable damage to the national security;
   b. never classify information to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment;
   c. distinguish, through portion marking and similar means, classified and unclassified information; and
   d. consider the public interest to the maximum extent feasible when making classification determinations, while continuing to protect information as necessary to maintain intelligence effectiveness, protect the safety of those who work for or with the IC, or otherwise protect national security.

4. Align IC roles, resources, processes, and policies to support robust implementation of these principles, consistent with applicable laws, executive orders, and directives.

Factors Affecting IC Performance: *Accomplishments, Risks, and Challenges*

The IC is an increasingly integrated intelligence enterprise working toward the common vision of a Nation made more secure by a fully integrated, agile, resilient, and innovative IC that exemplifies America's values. To this end, the IC has made significant accomplishments towards NIS objectives, but much work remains.

Accomplishments

Through integration of effort, workforce initiatives, IC partnerships, transparency, and technological innovation, IC leaders and managers have promoted a more efficient, effective, and agile intelligence enterprise that enables the United States to safeguard our national interests in a challenging world.

Intelligence Integration

Increased intelligence integration has enabled the IC to better optimize mutually supporting collection and analysis activities, and more effectively manage its resources, resulting in intelligence support that has been critical to successful military, diplomatic, humanitarian, and other relevant operations. Examples of integrated IC mission successes include the monitoring of the Iran nuclear program, the investigation of downed Malaysian Airlines Flight MH-17, the monitoring of North Korean nuclear weapons development, and the response to the Ebola virus outbreak in West Africa.

IC Workforce

IC mission success is enabled by an inclusive work environment and a talented and diverse workforce with opportunities to cultivate career growth through a continued focus on developing and leveraging diversity. As a result, the IC has consistently been ranked at the top of the best places to work in the Federal Government.

Through the IC Joint Duty Program, thousands of civilian personnel have gained expertise, serving alongside their colleagues in partner agencies, broadening their professional development, enhancing collaboration and information sharing, and promoting transparency and cooperation. Through this enriching program, our intelligence professionals have grown and gained additional experience and expertise and helped accomplish the IC's mission.

IC Partnerships

Significant progress has been made in building capacity, standardizing practices, and sharing information with partners in and outside the United States to help defend against and respond to foreign and foreign-inspired threats to U.S. interests, both at home and abroad. The IC advanced intelligence sharing with foreign partners, notably in countering terrorism and supporting military operations, and engaged in intelligence sharing activities with key domestic partners.

Transparency

The *Principles of Intelligence Transparency for the IC* facilitated decisions on making information publicly available to promote general understanding of intelligence activities, while continuing to protect information when disclosure would harm national security. As a result, the IC established a publicly available online repository for declassified documents, official statements, speeches, and testimony and has officially released thousands of pages of documents and posted them in this repository.

Technological Innovation

By deploying new scientific discoveries and technologies, nurturing innovative thought, and improving tradecraft and processes, the IC has

achieved greater mission advantage on important issues. For example, IC leaders and managers have promoted a culture of collaboration and integration along with unification of intelligence activities to deliver shared IT services and capabilities across the IC. This integrated approach will enable the IC to appropriately access information and tools, regardless of where in the IC they reside. Information that is better organized and enriched by metadata will enable the transition to information-centered intelligence processes, while streamlining integrated data, applications, and services.

A pioneering program has developed new methods for generating accurate and timely probabilistic forecasts on a wide range of intelligence questions. These forecasts have been used for National Intelligence Estimates and other intelligence products. To improve tradecraft, machine learning research has led to new automated methods for forecasting political instability from social media, news, financial data, web search queries, and thousands of other data streams. These innovative applications are beginning to revolutionize the future of intelligence to better inform our decisionmakers.

Risks and Challenges

The NIS addresses various sources of risk and challenges that IC elements are called upon to mitigate. Risk is an uncertain event or condition that has a negative effect on the IC's ability to accomplish its mission. Risk factors may have internal (areas the IC can control) and/or external (areas beyond the IC's control) causes, requiring tailored mitigation strategies.

- Strategic risk refers to factors that affect the IC's ability to provide sufficient intelligence to inform decisions on national security issues. Factors such as potentially degraded operational environments and the number and complexity of national security threats, together with resource constraints, may challenge the IC's ability to fully monitor situations and warn policymakers of all developments. The IC needs to pursue new approaches to better identify and communicate areas to accept risk while maintaining an anticipatory and agile posture against emerging threats.

- Institutional risk refers to the factors that affect the IC's ability to execute effective mission and business management practices. For example, the likelihood of future unauthorized disclosures is a known risk that, if realized, may negatively affect intelligence collection, relations with domestic and foreign partners, and public trust. Better governance, auditing, and security procedures are needed to mitigate the risk and minimize the impact. The IC must attract and retain the right, trusted, agile workforce that possesses skills such as the critical analytic, scientific, technological, engineering, math, cyber, and foreign language skills required to support current and future mission challenges. This includes continuing to make progress recruiting and hiring a more diverse workforce more comparable to external benchmarks, such as those of the Federal workforce, the private sector workforce, and the U.S. population.

- Programmatic (fiscal) risk refers to the consequences of losing IC capabilities and resources due to unplanned or unforeseen factors that impact the effective use of available funds. Continued federal budget uncertainty strains the IC's ability to make deliberative and responsive resource decisions. The outcome may be overextended budgets or lack of cost-effective solutions to address intelligence issues. The IC needs to develop methods to efficiently shift resources to mitigate programmatic (fiscal) risk and avoid loss of vital programs, capabilities, and resource investments.

- Technological risk refers to the factors that affect the IC's scientific and innovative methods, practices, tools, and skills. Some factors are known, while others may be unforeseen. An inability to stay current with rapid changes in technology and industry standards may affect the IC's competitive advantage. Mitigation may require improving data strategies, software, and infrastructure to retain state-of-the-art capabilities.

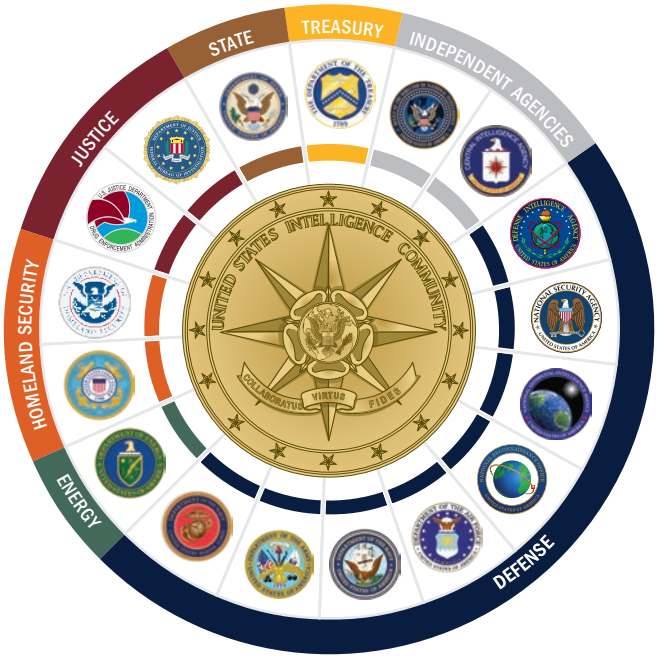
Organization of the Intelligence Community

The Intelligence Community is an integrated enterprise comprised of 17 Executive Branch agencies and organizations (generally referred to as "IC elements") that conduct a variety of intelligence activities and work together to promote national security. The DNI is the leader of the IC and sets IC strategic priorities through the National Intelligence Strategy. Each IC member contributes through the execution of its organization's mission in accordance with statutory responsibilities.

The IC is comprised of the following 17 elements:

- Two independent agencies – the Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA);
- Eight Department of Defense elements – the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and the intelligence and counterintelligence elements of the military services—U.S. Air Force Intelligence, U.S. Navy Intelligence, U.S. Army Intelligence, and U.S. Marine Corps Intelligence, which also receive guidance and oversight from the Under Secretary of Defense for Intelligence (USDI).
- Seven elements of other departments and agencies – the Department of Energy's Office of Intelligence and Counterintelligence; the Department of Homeland Security's Office of Intelligence and Analysis and the intelligence and counterintelligence elements of the U.S. Coast Guard; the Department of Justice's Federal Bureau of Investigation and the Drug Enforcement Administration's Office of National Security Intelligence; the Department of State's Bureau of Intelligence and Research; and the Department of the Treasury's Office of Intelligence and Analysis.

In addition to collection, analysis, and production, IC elements serve in other roles. Functional managers oversee and coordinate a specific intelligence discipline or capability and advise the DNI on the performance of their functions within and across IC elements. National Intelligence Managers serve as the DNI's principal advisers on all aspects of intelligence collection, analysis, and counterintelligence against a specific area of concern. Program managers are IC element heads responsible for executing the mission and overseeing their elements' budget activities. IC enterprise managers align capabilities and business functions to enable the mission.



Implementing the National Intelligence Strategy

The DNI, through the Office of the Director of National Intelligence, provides the IC with overarching oversight, direction, guidance, and coordination. IC elements execute their missions consistent with their statutory authorities. All members of the IC workforce are responsible for understanding how they contribute to the mission of the IC and executing their specific role to the best of their ability, while safeguarding privacy and civil liberties and practicing appropriate transparency.

DNI

Drive the Strategic Direction for the IC.

Through the NIS, the DNI sets strategic direction for the IC, bringing together the IC elements to address challenges that individual elements cannot solve on their own. The DNI provides direction for establishing and sustaining capabilities to enable mission success.

Lead Intelligence Integration. Under the direction of the DNI, the core mission of the ODNI is to lead and support IC integration; delivering insights, driving capabilities, and investing in the future. IC governance is the management of mission and enterprise activities through intelligence integration. Intelligence integration means coordinating and synchronizing collection, analysis, and counterintelligence so that they are fused, effectively operating as one team. The DNI establishes policies and standards to enable intelligence integration.

Enable IC Mission Execution. The DNI leads IC mission execution through decisionmaking bodies, IC strategies, IC budget and resource management, development of IC capabilities, information sharing and safeguarding, and partnering with domestic and foreign partners.

Direct the IC's Budget. The National Intelligence Program (NIP) is the IC's budget. The NIS serves as the DNI's mechanism to align NIP resources and report resource expenditures and performance to Congress. The DNI leads an IC-wide effort to develop an integrated NIP budget, maintaining strategic focus and cross-IC budget awareness, to assure that NIP investments best support national security goals and objectives. The DNI also participates in the development of annual budgets for the Department of Defense IC elements under the Military Intelligence Program (MIP). The DNI serves as a voice and advocate for the IC to Congress and other external entities.

IC Elements

Align Strategies, Plans, and Actions. The NIS informs the strategic plans of the IC elements. The mission and enterprise objectives in the NIS shall be incorporated and cascaded into the strategies and plans of the IC elements. Functional managers, National Intelligence Managers, Program managers, and IC enterprise managers will align, synchronize, and integrate their activities to the NIS.

Inform Resource Allocation. Program managers are heads of IC elements responsible for executing the missions of the IC. They oversee their element's budget activities, make investments in capabilities, and execute expenditures within the NIP and the MIP in the IC budget process. Each year they provide a strategic program briefing to the DNI and report to Congress on their respective programs.

Assess Outcomes. Activities, initiatives, and operations addressing NIS mission and enterprise objectives require constant and consistent evaluation. IC elements will document the specific impact of their activities, initiatives and operations, the extent to which this impact contributes to broader NIS objectives, and any factors that impede their ability to advance NIS objectives. Measuring progress toward meeting NIS objectives is crucial to improving the overall performance of the IC.

Conclusion

The NIS provides the IC with the DNI's strategic direction for the next four years, aligns IC priorities with other national strategies, and supports the IC's mission to provide timely, insightful, objective, and relevant intelligence and support to inform national security decisions and to protect our Nation and its interests. The IC must fully reflect the NIS in agency strategic plans, annual budget requests, and justifications for the NIP. The DNI will assess IC element proposals, projects, and programs toward the objectives of the NIS to realize the IC's vision of a Nation made more secure by a fully integrated, agile, resilient, and innovative Intelligence Community that exemplifies America's values.

> *"We have to become much more agile, more innovative, more creative."*
>
> — Daniel R. Coats, *Director of National Intelligence*

PRINCIPLES of PROFESSIONAL ETHICS for the INTELLIGENCE COMMUNITY

As members of the intelligence profession, we conduct ourselves in accordance with certain basic principles. These principles are stated below, and reflect the standard of ethical conduct expected of all Intelligence Community personnel, regardless of individual role or agency affiliation. Many of these principles are also reflected in other documents that we look to for guidance, such as statements of core values, and the *Code of Conduct: Principles of Ethical Conduct for Government Officers and Employees*; it is nonetheless important for the Intelligence Community to set forth in a single statement the fundamental ethical principles that unite us and distinguish us as intelligence professionals.

MISSION We serve the American people, and understand that our mission requires selfless dedication to the security of our Nation.

TRUTH We seek the truth; speak truth to power; and obtain, analyze, and provide intelligence objectively.

LAWFULNESS We support and defend the Constitution, and comply with the laws of the United States, ensuring that we carry out our mission in a manner that respects privacy, civil liberties, and human rights obligations.

INTEGRITY We demonstrate integrity in our conduct, mindful that all our actions, whether public or not, should reflect positively on the Intelligence Community at large.

STEWARDSHIP We are responsible stewards of the public trust; we use intelligence authorities and resources prudently, protect intelligence sources and methods diligently, report wrongdoing through appropriate channels; and remain accountable to ourselves, our oversight institutions, and through those institutions, ultimately to the American people.

EXCELLENCE We seek to improve our performance and our craft continuously, share information responsibly, collaborate with our colleagues, and demonstrate innovation and agility when meeting new challenges.

DIVERSITY We embrace the diversity of our Nation, promote diversity and inclusion in our work force, and encourage diversity in our thinking.

The National Intelligence Strategy
of the United States of America

IC Vision *A Nation made more secure by a fully integrated, agile, resilient, and innovative Intelligence Community that exemplifies America's values.*

IC Mission *Provide timely, insightful, objective, and relevant intelligence and support to inform national security decisions and to protect our Nation and its interests.*

Customer Success

Our Customers

The President	National Security Council	Congress
Heads of Departments & Agencies of the Executive Branch	Chairman of the Joint Chiefs of Staff and senior military commanders	Others as the DNI determines appropriate
Warfighters, policymakers, diplomats, negotiators, and homeland security, law enforcement & international officials	Designated state, local, tribal, & territorial governments and first responders	

Mission Objectives

Strategic Intelligence
Enduring Interests

Current Operations Intelligence
Current and Planned Operations

Anticipatory Intelligence
Emerging Issues

- **Cyber Threat Intelligence**
- **Counterterrorism**
- **Counterproliferation**
- **Counterintelligence and Security**

Other Regional and Functional Issues

Enterprise Objectives

Integrated Mission Management

Integrated Business Management

- **People**
- **Innovation**
- **Information Sharing and Safeguarding**
- **Partnerships**
- **Privacy, Civil Liberties, and Transparency**