

The National Intelligence Strategy

of the United States of America

AUGUST 2009



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE AUG 2009		2. REPORT TYPE		3. DATES COVERED 00-00-2009 to 00-00-2009	
4. TITLE AND SUBTITLE The National Intelligence Strategy of the United States of America				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Office of the Director or National Intelligence National Intelligence Council, Washington, DC, 20005				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 24	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



The National Intelligence Strategy

August 2009



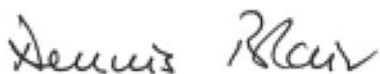
FOREWORD

Twenty years after the Berlin Wall came down and eight years after the tragedy of September 11, 2001, the United States has emerged from the post-Cold War world and post-9/11 world. We know the type of world we face, the nature of the threats, challenges, and opportunities before us, and the role intelligence can play in supporting policies that advance our national interests.

The United States faces a complex and rapidly shifting international security landscape. Events at home and abroad move quickly, often in an interconnected fashion, driven by the pace of technological change and international communications. National security priorities adapt as rapidly as these events unfold. The Intelligence Community (IC) must keep a steady focus on enduring challenges in and among nation-states and persistent transnational issues, and also be agile in adapting to emerging threats and harnessing opportunities. The *National Intelligence Strategy* (NIS) sets out the following guiding principles: responsive and incisive **understanding** of global threats and opportunities, coupled with an **agility** that brings to bear the Community's capabilities.

The 2009 NIS represents several advances in the Director of National Intelligence's (DNI) leadership of the National Intelligence Program (NIP) and the IC. It reflects a refined understanding of the counterterrorism challenge and elevates the importance of the challenges we face in the cyber domain and from counterintelligence threats. This NIS also affirms priorities to focus IC plans and actions for the next four years, while providing direction to guide development of future IC capabilities. The NIS highlights areas that demand our attention, resources, and commitment. It also establishes the basis for accountability, in conjunction with an implementation plan, to ensure that the Community meets the goals of our strategy.

This document affirms the vital role that intelligence plays in our Nation's security. We will only succeed because of the extraordinary talent, courage, and patriotism of our professionals.



Dennis C. Blair
Director of National Intelligence

VISION FOR THE INTELLIGENCE COMMUNITY

The United States Intelligence Community must constantly strive for and exhibit three characteristics essential to our effectiveness. The IC must be *integrated*: a team making the whole greater than the sum of its parts. We must also be *agile*: an enterprise with an adaptive, diverse, continually learning, and mission-driven intelligence workforce that embraces innovation and takes initiative. Moreover, the IC must *exemplify America's values*: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people.



THE STRATEGIC ENVIRONMENT

The United States faces a complex and rapidly changing national security environment in which nation-states, highly capable non-state actors, and other transnational forces will continue to compete with and challenge U.S. national interests. Adversaries are likely to use asymmetric means and technology (either new or applied in a novel way) to counter U.S. interests at home and abroad. There may be opportunities for cooperative multilateral action to meet these challenges.

A number of **nation-states** have the ability to challenge U.S. interests in traditional (e.g., military force and espionage) and emerging (e.g., cyber operations) ways.

- **Iran** poses an array of challenges to U.S. security objectives in the Middle East and beyond because of its nuclear and missile programs, support of terrorism, and provision of lethal aid to U.S. and Coalition adversaries.
- **North Korea** continues to threaten peace and security in East Asia because of its sustained pursuit of nuclear and ballistic missile capabilities, its transfer of these capabilities to third parties, its erratic behavior, and its large conventional military capability.

- **China** shares many interests with the United States, but its increasing natural resource-focused diplomacy and military modernization are among the factors making it a complex global challenge.

- **Russia** is a U.S. partner in important initiatives such as securing fissile material and combating nuclear terrorism, but it may continue to seek avenues for reasserting power and influence in ways that complicate U.S. interests.

There also may be opportunities for cooperation with many nation-states, including those cited above, in support of common interests that include promoting rule of law, representative government, free and fair trade, energy, and redress of troublesome transnational issues.

Non-state and sub-state actors increasingly impact our national security.

- **Violent extremist groups** are planning to use terrorism—including the possible use of nuclear weapons or devices if they can acquire them—to attack the United States. Working in a number of regions, these groups aim to derail the rule of law, erode societal order, attack U.S. strategic partners, and otherwise challenge U.S. interests worldwide.
- **Insurgents** are attempting to destabilize vulnerable states in regions of strategic interest to the United States.

- **Transnational criminal organizations**, including those that traffic drugs, pose a threat to U.S. interests by potentially penetrating and corrupting strategically vital markets; destabilizing certain nation-states; and providing weapons, hard currency, and other support to insurgents and violent criminal factions.

A number of **transnational forces and trends**—from shifting global demographics to resource struggles—present strategic challenges to U.S. interests, but also provide new opportunities for U.S. global leadership.

- The **global economic crisis** could accelerate and weaken U.S. security by fueling political turbulence. In some developing economies, a sustained slowdown could induce social and political instability, while in others it could erode support for market-oriented liberal democracy and create openings for authoritarianism.
- **Failed states and ungoverned spaces** offer terrorist and criminal organizations safe haven and possible access to weapons of mass destruction (WMD), and may cause or exacerbate starvation, genocide, and environmental degradation.

- **Climate change and energy competition** may produce second-order effects for national security as states anticipate the effects of global warming (e.g., by contesting water resources in regions with limited potable sources) and seek to secure new energy sources, transport routes, and territorial claims.

- Rapid **technological change** and dissemination of information continue to alter social, economic, and political forces, providing new means for our adversaries and competitors to challenge us, while also providing the United States with new opportunities to preserve or gain competitive advantages.

- As the 2009 H1N1 influenza outbreak vividly illustrates, the risk of **pandemic disease** presents a persistent challenge to global health, commerce, and economic well-being.



GOALS AND OBJECTIVES

The Intelligence Community has four strategic goals. In order to meet them, we must operate effectively regardless of where the intelligence resides, with a clear legal framework to guide us. The first two goals, supported by six Mission Objectives (MOs), speak to the missions we must accomplish. The third and fourth goals, supported by seven Enterprise Objectives (EOs), describe what we will achieve as an intelligence enterprise to support our Mission Objectives.

- **Enable wise national security policies** by continuously monitoring and assessing the international security environment to warn policymakers of threats and inform them of opportunities. We will provide policymakers with strategic intelligence that helps them understand countries, regions, issues, and the potential outcomes of their decisions. We will also provide feedback to policymakers on the impact of their decisions.
- **Support effective national security action.** The IC will deliver actionable intelligence to support diplomats, military units, interagency organizations in the field, and domestic law enforcement organizations at all levels. At times, we will be directed by the President to carry out covert activities that we will faithfully execute within the bounds of U.S. law.

- **Deliver balanced and improving capabilities** that leverage the diversity of the Community's unique competencies and evolve to support new missions and operating concepts. We must integrate Community capabilities to reap synergies and efficiencies, continuously reassessing and adjusting our portfolio so that we can prepare for tomorrow's challenges while performing today's missions.
- **Operate as a single integrated team,** employing collaborative teams that leverage the full range of IC capabilities to meet the requirements of our users, from the President to deployed military units.

Mission Objectives

- MO1: Combat Violent Extremism
- MO2: Counter WMD Proliferation
- MO3: Provide Strategic Intelligence and Warning
- MO4: Integrate Counterintelligence
- MO5: Enhance Cybersecurity
- MO6: Support Current Operations

Enterprise Objectives

- EO1: Enhance Community Mission Management
- EO2: Strengthen Partnerships
- EO3: Streamline Business Processes
- EO4: Improve Information Integration & Sharing
- EO5: Advance S&T/R&D
- EO6: Develop the Workforce
- EO7: Improve Acquisition

MISSION OBJECTIVES

MO 1: Combat Violent Extremism

Understand, monitor, and disrupt violent extremist groups that actively plot to inflict grave damage or harm to the United States, its people, interests, and allies.



Violent extremist groups—primarily al-Qa’ida and its regional affiliates, supporters, and the local terrorist cells it inspires—will continue to pose a grave threat to U.S. persons and interests at home and abroad.

The Intelligence Community supports the whole-of-U.S. Government efforts to protect the homeland, defeat terrorists and their capabilities, counter the spread of violent extremism, and prevent terrorists from acquiring or using weapons of mass destruction. The IC’s mission is to identify and assess violent extremist groups; warn of impending attacks; and develop precise intelligence to cut off these groups’ financial support and to disrupt, dismantle, or defeat their operations.

We will build on the IC’s significant progress since September 11, 2001. We must continue improving our capabilities to enhance the quality of our support and the responsiveness to customers’ needs.

- **Provide warning.** Provide timely and actionable warning of terrorist attacks.
- **Disrupt plans.** Penetrate and support the disruption of terrorist organizations and the nexus between terrorism and criminal activities.
- **Prevent WMD Terrorism.** Support U.S. efforts to prevent terrorists’ acquisition and use of weapons of mass destruction.
- **Counter radicalization.** Identify terrorists’ radicalization efforts and provide opportunities for countering violent extremism.

MO 2: Counter WMD Proliferation

Counter the proliferation of weapons of mass destruction and their means of delivery by state and non-state actors.



The Intelligence Community must support five enduring policy objectives for countering the proliferation of WMD and their means of delivery: dissuade, prevent, roll back, deter, and manage consequences. The IC will work with partners inside and outside the U.S. Government to improve capabilities needed to support action across all five WMD objectives.

The IC must continue enhancing its capabilities in the following areas:

- **Enhance dissuasion.** Identify opportunities and levers that the United States and its allies can use to discourage interest in WMD.
- **Support prevention.** Increase support to policymakers in preventing WMD proliferation by enhancing capabilities that contribute to U.S. Government efforts to prevent the flow of WMD-related materials, technologies, funds, and expertise.
- **Enable rollback.** Identify opportunities and levers that the United States and its allies can use to end or roll back WMD or capabilities that raise serious concerns.
- **Enhance deterrence.** Improve capabilities to understand adversaries' WMD plans, intentions, and doctrines and to deny the impact of their capabilities.
- **Manage consequences.** Reinforce U.S. Government efforts to mitigate or manage the consequences of WMD use by supporting the characterization of adversaries' WMD capabilities and the development of countermeasures against WMD use, and by improving the ability to support timely attribution of WMD used against the United States, its allies, or friends.

MO 3: Provide Strategic Intelligence and Warning

Warn of strategic trends and events so that policy-makers, military officials, and civil authorities can effectively deter, prevent, or respond to threats and take advantage of opportunities.



imagebroker/Alamy

The issues and trends that will shape the future security environment—economic instability, state failure, the ebb and flow of democratization, emergence of regional powers, changing demographics and social forces, climate change, access to space, pandemic disease, and the spread of disruptive technologies, to name just a few—will test the Intelligence Community's ability to provide strategic warning and avoid surprise. Most of the IC's analytic cadre focus on assessing ongoing and near-term events of significance. The IC must improve its ability to anticipate and identify emerging challenges and opportunities.

To accomplish this objective, the Community must better integrate long-range and trend analysis, strategic warning, and opportunity identification. This will enable multiple objectives, including long-range policy planning, strategy development, and policy formulation. We must identify the gaps in our knowledge

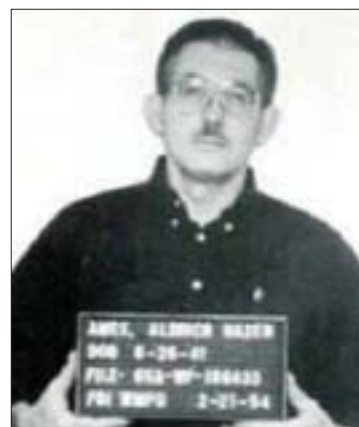
on the Nation's highest priorities to focus analysis, drive collection strategies, and produce deep insight. We must continuously review and adjust Community analytic resources, capabilities, tradecraft, and performance to ensure proper coverage of strategic analytic priorities. Expanded use of techniques such as red-teaming can help ensure quality and integrity in analytic products, and potentially produce fresh insights into our toughest challenges.

In particular, the IC must:

- **Broaden expertise.** Provide greater scope, depth, and quality of intelligence analysis—especially in economics, energy and natural resources, and non-military technologies.
- **Deepen understanding.** Build and access deep understanding of the cultural, political, religious, economic, ethnic, and tribal factors in operational theaters.
- **Enhance outreach.** Conduct strategic outreach to key external centers of knowledge and expertise.
- **Improve collaboration.** Develop and field new techniques and capabilities to enhance collaboration and promote a Community-wide culture of sound strategic analysis.
- **Increase language skills.** Increase the quantity and fluency of our foreign language capability.

MO 4: Integrate Counterintelligence

Provide a counterintelligence capability that is integrated with all aspects of the intelligence process to inform policy and operations.



Foreign entities, including state and non-state actors, violent extremist groups, cyber intruders, and criminal organizations, are increasingly undermining U.S. interests in myriad and growing ways. Globalization of the marketplace and the openness of modern information networks have enabled our adversaries' goals. At the strategic level, these actors are attempting to manipulate U.S. policy and diplomatic efforts, disrupt or mitigate the effectiveness of our military plans and weapon systems, and erode our economic and technological advantage. At the tactical level, they are intent on penetrating our critical infrastructure, information systems, and leading industries.

Our counterintelligence (CI) community must lead a consistent, comprehensive, and collaborative effort across the U.S. Government, employing both offensive and defensive CI measures to identify, deceive, exploit, disrupt, and protect against these threats. The CI community must serve both the policymaker

and operator. Tasks include: penetrating and exploiting adversaries, mitigating the insider threat, providing input to strategic warning, validating sources of intelligence, contributing to cyber defense, and evaluating acquisition risk.

Our CI community must build on its current efforts and focus in four areas:

- **Detect insider threats.** Detect insiders who seek to exploit their authorized access in order to harm U.S. interests.
- **Penetrate foreign services.** Penetrate hostile foreign intelligence services to determine their intentions, capabilities, and activities.
- **Integrate CI with cyber.** Employ CI across the cyber domain to protect critical infrastructure.
- **Assure the supply chain.** Assure the national security community's supply chain from foreign intelligence exploitation.

MO 5: Enhance Cybersecurity

Understand, detect, and counter adversary cyber threats to enable protection of the Nation's information infrastructure.



The architecture of the Nation's digital infrastructure, based largely upon the Internet, is neither secure nor resilient. Nation-states and non-governmental entities are compromising, stealing, changing, or destroying information, and have the potential to undermine national confidence in the information systems upon which our economy and national security rests. The Intelligence Community plays an integral role in enhancing cybersecurity both by increasing our ability to detect and attribute adversary cyber activity and by expanding our knowledge of the capabilities, intentions, and cyber vulnerabilities of our adversaries.

The IC has made progress in implementing the initiatives and developing the enabling capabilities needed to meet national cybersecurity guidance. We must quickly add to these efforts through the following:

- **Leverage partnerships.** Integrate cyber expertise throughout the IC, as well as with allied intelligence services, industry, and the academic community.
- **Protect U.S. infrastructure.** Identify, prioritize, and close the gaps in our collection capability and analytic knowledge base on threats to our cybersecurity.
- **Combat cyber threats to non-traditional targets.** Focus more resources on identifying and neutralizing cyber threats to non-traditional intelligence customers.
- **Manage the cyber mission.** Strengthen Community-wide processes for mission management, specifically processes for enabling collaborative planning and execution and for providing a scalable, foundational capability to conduct cyber operations.

MO 6: Support Current Operations

Support ongoing diplomatic, military, and law enforcement operations, especially counterinsurgency; security, stabilization, transition, and reconstruction; international counternarcotics; and border security.



Scott Peterson/Getty Images

Intelligence will continue to be a critical factor in a range of ongoing missions: defeating the Taliban in Afghanistan, stabilizing Iraq, curbing drug cartels, ensuring the free and lawful flow of people and goods into and out of the homeland, and dealing with new contingencies as they arise. These ongoing operations have greatly expanded the Intelligence Community's missions and placed heavy demands on its resources and analytic efforts.

The IC has made notable progress in bringing actionable intelligence to bear in multiple complex and dangerous environments. However, we need to

continue to develop new approaches; eliminate or reduce barriers to efficiency and effectiveness; and sustain technical, analytic, linguistic, and operational excellence to support a wide range of military, law enforcement, and civilian operations. We must also continue to improve our ability to collaborate between intelligence and law enforcement to detect and respond to threats to the homeland. Three areas deserve focus:

- **Monitor time-sensitive targets.** Sustain multi-discipline, high-fidelity collection on, and analysis of, time-sensitive targets.
- **Forward deploy collection and analytic presence.** Embed Community analysts in operational settings as part and parcel of an integrated enterprise approach.
- **Share information.** Enhance the ability to share intelligence with foreign governments; federal civil agencies; and state, local, tribal, and private-sector partners.

ENTERPRISE OBJECTIVES

EO 1: Enhance Community Mission Management

Adopt a mission approach as the expected construct for organizing and delivering intelligence support on high-priority challenges.



The IC is at its best when it integrates its efforts across the enterprise to meet specific mission needs. Mission management provides a mechanism for focusing Community efforts against missions of high priority; it does not direct agencies how to perform their functions. Mission management leadership brings greater integration of analysis and collection so that priority intelligence gaps are identified, integrated solutions are developed and executed, and additional insights are provided to analysts, policy-makers, and operators.

We must capture the best practices of mission management from recent years, find ways to nurture their development, integrate them across the Community, and encourage Community leadership at all levels to take the initiative and apply these practices. Mission management must be the norm, not the exception, for approaching our most important challenges.

The principles of Community mission management are:

- **Create unity of effort.** Work together, under common direction, as integrated, cross-cleared, multi-intelligence discipline teams to ensure the full range of IC capabilities are marshaled against the challenge. Community mission management leads to unified strategies that identify required actions, resources, and policies needed to accomplish the mission. IC elements are collaborative partners that share information, capabilities, and resources to achieve mission success.
- **Ensure accountability.** Designate an individual, team, center, or executive agency to act on the DNI's behalf to manage a national-level mission for the Community.
- **Tailor support.** Allow mission management to take many forms. We require a flexible approach that allows tailored support where no single solution fits all. Some forms of mission management require establishing a major center with a large staff, similar to the National Counterterrorism Center; others can be less formal, smaller arrangements similar to the Strategic Interdiction Group.
- **Foster agility.** Inculcate a mission approach in all we do and encourage initiative at all levels in response to mission needs. Our construct must allow the IC to respond to complex challenges of highest national importance, including ones that arise suddenly and that require extraordinary effort from across the Community. The mission centers must move quickly to identify and meet intelligence needs, stay in touch with a wide range of policy and operational organizations, and provide timely and relevant intelligence support.

- **Deepen relationships.** Foster intense interactive links with users, whether they are policymakers or operators in the field. Mission centers must have direct relationships with users, while keeping IC components and the Office of the Director of National Intelligence (ODNI) informed of developments and requirements.
- **Foster mission management.** Establishing mission teams for complex challenges often requires significant changes in assignments, tasking, analytic production, and information-sharing arrangements. The IC must work cooperatively to encourage leaders at all levels to adopt a mission management approach, ensure that mission teams have the institutional support and resources needed, and continually review the impact of establishing such teams or centers and the gains achieved through doing so.

EO 2: Strengthen Partnerships

Strengthen existing and establish new partnerships with foreign and domestic, public and private entities to improve access to sources of information and intelligence, and ensure appropriate dissemination of Intelligence Community products and services.



The IC must leverage partnerships to obtain the access, expertise, and perspective required to succeed at our missions. Partnerships are particularly important for transnational issues that cross traditional organizational lines. In some cases, this means deepening existing traditional liaison relationships; in others, forging non-traditional relationships.

Our approach must align with broader national policy and be harmonized across the IC through policy that delineates roles, responsibilities, and authorities. Partnerships vary in scope, depth, and duration to reflect the type of requirement, the expected benefits, and the anticipated risks. Partnership characteristics may also vary across mission area, time, and intensity. To address these multiple and sometimes conflicting demands, we will identify and prioritize which partnerships to form, when and under what conditions; coordinate IC interaction to advance common goals and use resources optimally; and assess the effectiveness of partnerships individually and collectively and adjust them accordingly.

To enhance our partnerships, we must focus in the following areas:

- **Build familiarity.** Deepen partners' knowledge of the IC and its capabilities and capacity, as well as IC understanding of the benefits partners provide.

- **Expand partnerships.** Codify new relationships with a variety of partners, and between the partners themselves, to drive collaboration and information sharing.
- **Establish new partnerships.** Build mutual trust and a shared understanding of needs, capabilities, and missions with partners, particularly those with whom the IC has traditionally not had a relationship.

EO 3: Streamline Business Processes

Streamline IC business operations and employ common business services to deliver improved mission support capabilities and use taxpayer dollars more efficiently and effectively.



The Intelligence Community faces several critical challenges related to its business and security systems environments: redundant and non-interoperable systems and infrastructure; the inability to achieve clean financial audits as a result of poor data quality and integrity; and disparate, inefficient, ill-defined business and security clearance processes with

unclear outcomes. We need more timely access to critical information, as well as easier aggregation of specific information at the enterprise level.

To address these challenges, eliminate wasteful redundancies, and transform enterprise business and security operations, the Intelligence Community must:

- **Modernize business operations.** Transform business operations and processes using innovative approaches, collaborative fora, and recognized best practices that inform senior IC leaders of the status of critical assets and issues.
- **Adopt standards and processes.** Develop and employ enterprise business standards and processes, modernize operations and services, and improve them through established performance goals and targets.
- **Implement a shared business/mission environment.** Implement a shared environment with improved business operations and services that enhances mission capabilities and simplifies IC leader access to business information and optimizes use of taxpayer money.
- **Integrate security practices.** Ensure security practices are streamlined and then integrated into transformed business processes to protect national intelligence and intelligence sources and methods.

- **Demonstrate sound financial management.**

Achieve financial management transparency, accountability, and auditability, compliant with applicable laws and Office of Management and Budget (OMB) guidelines.

- **Promote robust consultation and oversight.**

Support effective consultation with, and oversight by, inspectors general, general counsels, and agency officials responsible for privacy and civil liberties protection, with respect to processes, operations, and services.

EO 4: Improve Information Integration & Sharing

Radically improve the application of information technology—to include information management, integration and sharing practices, systems and architectures (both across the IC and with an expanded set of users and partners)—meeting the responsibility to provide information and intelligence, while at the same time protecting against the risk of compromise.



The Intelligence Community faces an explosive growth in type and volume of data, along with an exponential increase in the speed and power of processing capabilities. Threats to our networks and the integrity of our information have proliferated. Our partners and users increasingly expect us to discover, access, analyze, and disseminate intelligence information in compressed time frames. We have the responsibility to share information, while protecting sources and methods and respecting the privacy and rights of U.S. citizens.

Information policies, processes, and systems must cope with these circumstances, while providing a trusted and reliable environment to support operations, even when under attack. Initiatives and programs tied to information sharing and systems must accelerate and synchronize delivery of information enterprise capabilities. In addition, we must keep pace with changes in technology and mission needs. The Community must focus on the following areas:

- **Assure the environment.** Develop a world-class, Community-wide, assured information environment based on a common, effective, reliable, and secure infrastructure capable of providing information wherever IC elements or their customers are positioned.
- **Rationalize solutions.** Enable the rapid implementation of simple, logical, effective, cross-cutting solutions (materiel and non-materiel), recognizing the need to terminate and eliminate legacy systems.
- **Enable information flow.** Integrate assured and authorized discovery and access of information to the IC workforce, while ensuring timely and

tailored dissemination of information at appropriate classification levels.

- **Improve information aggregation and analysis.** The IC must narrow the gap between our capacity to “sense data” and our capabilities to “make sense of data” in handling an exponentially increasing volume and variety of data and information.
- **Maintain cyber security awareness.** Improve cyber security awareness and training throughout the IC enterprise, including IC partners and customers.

EO 5: Advance S&T/R&D

Discover, develop, and deploy Science & Technology/Research & Development advances in sufficient scale, scope, and pace for the IC to maintain, and in some cases gain, advantages over current and emerging adversaries.



The explosive pace in the development of technology offers opportunities to improve the IC’s productivity, effectiveness, and agility even if its increasing availability may also benefit our adversaries. History proves that riding the leading edge of technology is critical to the IC’s ability to deliver better intelligence.

The focus of the IC’s Science & Technology (S&T) enterprise rests on several factors. Our adaptation, adoption, and development of technology will be guided by a combination of “technology push,” “capabilities pull,” and “mission pull.” The range of missions we face demands innovative approaches in many areas, from major long-term collection systems to advanced analytical techniques, and clandestine sensors to secure, reliable networks and communications systems. Our Research & Development (R&D) program must balance the larger, longer-term, and often higher-risk initiatives that promise dramatically improved or completely unexpected capabilities with smaller, incremental improvements in capability that can be brought into use rapidly, then adapted and improved as they are used.

We must coherently manage the S&T/R&D effort across the IC to accelerate technology development, enhance collaboration, develop new and unexpected solutions, and protect “high risk/big payoff” projects such as those in the Intelligence Advanced Research Projects Activity. Other specific areas of focus include:

- **Transition new technologies.** Improve the transition of S&T solutions to the operational user and into major system acquisition, as appropriate.
- **Expand partnerships.** Engage the academic community, industry, U.S. and partner-nation governments, mission customers, and non-governmental centers of technical excellence and innovation.

- **Scan for trends.** Assess global technology trends to find emerging and potential breakthroughs and new technology for integration into IC capabilities.

EO 6: Develop the Workforce

Attract, develop, and retain a diverse, results-focused, and high-performing workforce capable of providing the technical expertise and exceptional leadership necessary to address our Nation's security challenges.



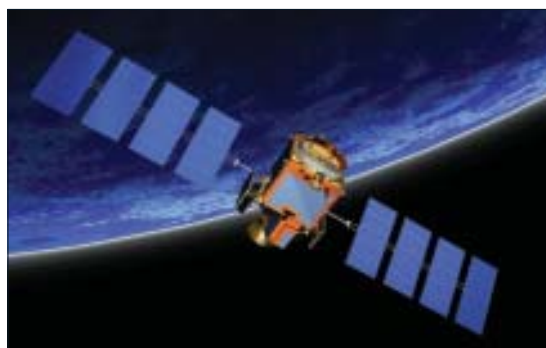
People are at the core of building an agile and flexible intelligence enterprise and promoting a culture of collaboration. We must continue to build a diverse workforce with technical, linguistic, and cultural understanding and expertise that can work across organizational boundaries and meet the wide-ranging requirements of our mission objectives.

To meet this objective, the Community must:

- **Build a diverse and balanced workforce.** Employ, develop, and retain a workforce that reflects diversity in its broadest context—culture, ethnicity, ancestry, race, gender, language, and experiences—properly balanced among its military, civilian, and contractor components.
- **Enhance professional development.** Develop, reward, and retain technical expertise and professional leadership, including in S&T.
- **Cultivate relevant expertise.** Educate and train the workforce to align with national security and intelligence priorities.
- **Support an entrepreneurial ethos.** Encourage initiative, innovation, collaboration, resourcefulness, and resilience.
- **Deploy integrated, agile teams.** Integrate and deploy cross-functional and cross-organizational teams of personnel to meet mission objectives.
- **Build a culture of leadership excellence.** Create and sustain a culture of personal, professional, technical, and managerial leadership at all organizational levels.

EO 7: Improve Acquisition

Improve cost, schedule, performance, planning, execution, and transparency in major system acquisitions, while promoting innovation and agility.



Acquisition excellence requires a combination of agile decisionmaking and disciplined execution to leverage technology while meeting cost, schedule, and performance expectations. Major system acquisitions provide important new capabilities to meet future missions. Being able to deliver capability cost-effectively when it is needed improves mission effectiveness, provides leadership with flexibility in making investments, and precludes gaps in necessary capabilities.

Acquisition delivery timelines must be shortened to allow for innovation and maximum exploitation of new technologies. Agile decisionmaking and disciplined execution require that we:

- **Develop qualified acquisition professionals.** Provide expertise in leading the planning and execution of major IC acquisition programs. The IC acquisition workforce must be experienced, educated, and trained in the best practices of acquisition by parent organizations, with support from the ODNI.
- **Employ effective acquisition processes.** Apply the best practices of systems engineering, contracting, technology maturation, cost estimating, and financial management in acquisition execution. IC elements must demonstrate discipline in documenting and executing these processes. The ODNI will ensure that the best practices are applied across the Community.
- **Align with complementary processes.** Synchronize the planning, programming, and execution of major acquisition programs with other IC and Department of Defense processes. The requirements process must generate clearly defined user expectations; cost estimates must better align with the development of the annual budget; and human resources processes must provide personnel needed for successful execution.
- **Empower decisionmaking at lower levels.** Empower acquisition executives and program managers to manage programs and be held accountable for the results. In order to streamline decisionmaking, the DNI will delegate statutory milestone decision authority to the maximum extent possible when IC elements demonstrate a track record of successful performance, maintain transparency, and freely provide information to oversight entities.

ROLE OF THE DNI IN IMPLEMENTING THE NIS

By law and executive order, the DNI has sole authority to lead the Intelligence Community and manage the NIP. A principal vehicle through which the DNI executes responsibility on behalf of the President and the National Security Council is the *National Intelligence Strategy*. The DNI's role in leading the Community to implement the NIS includes:

- **Establish priorities with clear and measurable goals and objectives.** The DNI sets the intelligence agenda. The DNI will translate user requirements into intelligence priorities by which IC resources can be managed and progress measured and assessed.
- **Provide leadership on cross-cutting issues.** The DNI will exercise leadership to align incentives and enforce compliance on the coordination of issues that cross IC organizational boundaries.
- **Set direction through policy and budgets.** The DNI will issue policy directives to clarify roles and responsibilities so IC elements can effectively carry out NIS goals and objectives. Of particular importance is policy that enables or induces collaboration to meet DNI direction. The DNI will also determine the NIP budget request to the President and oversee execution of budgetary resources to properly fund national-level priorities.



- **Promote integration of agency capabilities.** The DNI will promote a “joint” perspective for how capabilities can be combined or integrated to achieve synergies and efficiencies so that the sum of the IC is greater than its parts. While some natural alignment occurs, the DNI has particular interest in reducing unwanted or unnecessary redundancy and increasing our shared effectiveness.
- **Monitor agency and leadership performance.** The DNI will establish and enforce performance expectations by reviewing IC elements’ strategic plans for alignment with the NIS, assessing element and IC-wide progress against NIS objectives, and ratifying personal performance agreements that specify how the IC elements’ leaders are accountable for implementing the NIS.

IC components have a similar responsibility to develop plans, capabilities, programs, and policies that explicitly support the objectives laid out in this strategy.

CONCLUSION

The *National Intelligence Strategy* presents a way ahead for the Intelligence Community to focus on the missions the Nation requires, enhance the enterprise’s agility, and improve understanding and support to our users. We must now translate this strategy into initiatives, plans, and capabilities. Decisions about program, budgeting, policy, and acquisition, as well as the operation of the IC, will reflect this document. The objectives in this NIS shall be incorporated into the Intelligence Planning Guidance and cascaded into direction given for development of integrated program and budget options and recommendations. The development of measures and targets for the NIS’s objectives will ensure we can assess our progress and adapt our approach during implementation as appropriate. Only as we become a unified enterprise can we meet the unprecedented number of challenges we face and seize opportunities to enhance the security of the United States along with that of its allies, friends, and like-minded nations.



The Office of the Director of National Intelligence