National Intelligence Strategy

2023

From the Director of National Intelligence

Following the attacks of September 11, 2001, and in the wake of the Intelligence Reform and Terrorism Prevention Act passed by Congress in 2004, Director of National Intelligence John D. Negroponte signed out the Intelligence Community's (IC) first National Intelligence Strategy. The strategy explained that the Intelligence Community's clear charge was to:

- Integrate the domestic and foreign dimensions of U.S. intelligence so that there are no gaps in our understanding of threats to our national security;
- Bring more depth and accuracy to intelligence analysis; and
- Ensure that U.S. intelligence resources generate future capabilities as well as present results.

Now, almost twenty years after our first strategy was issued, the Intelligence Community's charge remains just as clear, even as the strategic environment has changed dramatically. The United States faces an increasingly complex and interconnected threat environment characterized by strategic competition between the United States, the People's Republic of China (PRC), and the Russian Federation, felt perhaps most immediately in Russia's ongoing aggression in Ukraine. In addition to states, sub-national and non-state actors—from multinational corporations to transnational social movements—are increasingly able to create influence, compete for information, and secure or deny political and security outcomes, which provides opportunities for new partnerships as well as new challenges to U.S. interests. In addition, shared global challenges, including climate change, human and health security, as well as emerging and disruptive technological advances, are converging in ways that produce significant consequences that are often difficult to predict.

As Director of National Intelligence, I have the privilege of leading an Intelligence Community that provides decision-makers and citizens crucial insights on this diverse and complex landscape. Our support to policymakers, operators, and warfighters is critically dependent on our ability to look beyond the immediate horizon to ensure the Intelligence Community is well postured to address emerging threats, promote national resilience and innovation, defend our competitive advantage, and promote shared prosperity. This National Intelligence Strategy, therefore, lays out the Intelligence Community's role in supporting the priorities outlined in the President's National Security Strategy and serves as the Community's direction for the next four years as we seek to better serve the Nation.

The six goals outlined in this National Intelligence Strategy have emerged as our understanding of the kinds of information, technology, and relationships needed to be effective in the future has expanded. Whether we are successful in achieving these goals will depend on whether we can maintain a talented and diverse workforce, and whether we can adapt, increase resilience, and sustain our focus on overcoming the challenges of a rapidly changing environment. I believe we have the capacity, will, and talent to do so.

Avril D. Haines
Director of National Intelligence

The National Intelligence Strategy of the United States of America

IC Vision

An Intelligence Community that embodies America's values and is sufficiently agile, integrated, innovative, and resilient to inform national security and foreign policy decisions, resulting in a Nation that is secure and prosperous.

IC Mission

The U.S. Intelligence Community provides timely, rigorous, apolitical, and insightful intelligence and support to inform national security decisions and protect our Nation and its interests.

Our success as a Community is measured as much by our defense of America's values as it is by the execution of our intelligence mission. The 2023 National Intelligence Strategy recognizes that a purposeful and clear set of ethics serves as a cornerstone of the United States Intelligence Community's mission.

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 workforce, and encourage diversity in our thinking.

GOAL 1

GOAL 1: Position the IC for Intensifying Strategic Competition

Strategic competition from powers that layer authoritarian governance with a revisionist foreign policy is a principal challenge to a free, open, secure, and prosperous world. The PRC is the only U.S. competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so. Russia poses an immediate and ongoing threat to the regional security order in Europe and Eurasia and is a source of disruption and instability globally, but it lacks the across-the-spectrum capabilities of the PRC.

Leadership in technology and innovation has long underpinned our economic prosperity and military strength, and will be critical to outcompeting our rivals, advancing our interests, and safeguarding democracy. The United States must be able to identify the applications and implications of emerging technologies, understand supply chains, and use economic statecraft tools—in coordination with our allies and partners—to ensure strategic competitors are not able to undermine our competitiveness and national security.

The IC must deepen and expand its expertise, strengthen its collection and analytic capabilities, and embrace new partnerships and external perspectives to address policymaker needs in this more competitive environment. The IC will invest in developing innovative methods and cultivating new sources, and work more systematically with allies and partners and public and private sector partners to facilitate a common understanding of technological and other risks and how to address them. Given the global nature of strategic competition, the IC will establish methods and systems that promote greater interoperability and understanding across traditional and distinct geographic and functional areas. These efforts are essential to the IC's success as a key element of national power in this competition.

The IC will improve its ability to provide timely and accurate insights into competitor intentions, capabilities, and actions by strengthening capabilities in language, technical, and cultural expertise and harnessing open source, "big data," artificial intelligence, and advanced analytics. The IC also must enhance its ability to understand how countries in every region of the world perceive, are implicated by, and seek to navigate this new landscape, and assess their opportunities to enhance strategic relationships with the United States. At the same time, the IC will improve its understanding of how non-state actors might use their growing resources and capacity to exert unilateral and collective influence in a way that could support or undermine U.S. national security. And above all else, the IC will use its authorities and capabilities in ways that strengthen our democratic foundations and principles as we seek to counter increasingly autocratic competitors.

GOAL 2

GOAL 2: Recruit, Develop, and Retain a Talented and Diverse Workforce that Operates as a United Community

The IC's future success depends on its ability to attract and retain a highly technical and talented workforce that draws on one of our country's unmatched reservoirs of strength: our diversity. Varied backgrounds, perspectives, and experiences strengthen our workforce, our ability to deliver on our Mission, and the trust of the American public.

The Community must overcome long-standing cultural, structural, bureaucratic, technical, and security challenges to reimagine and deliver the IC workforce of the future.

The IC will modernize recruiting, hiring, and vetting processes to ensure its ability to competitively and rapidly recruit and onboard a diverse, trusted, agile, and expert IC workforce. The IC will also build on efforts to implement continuous monitoring and security clearance reciprocity so the Community can operate in new ways, rapidly redistributing and better integrating expertise where and when it is most needed, taking advantage of greater workplace flexibilities, and leveraging skills from across the Community regardless of organizational affiliation.

Enhanced professional development opportunities at every level of the workforce are critical to building a shared strategic awareness of the IC's full capabilities, its missions, and its challenges and ensuring greater literacy and expertise in emerging disciplines and fields. The IC must also incentivize, reward, and offer opportunities for regular joint duty rotations to produce officers more capable of formulating holistic and integrated solutions to intelligence problems.

Diversity, equity, inclusion, accessibility, and other human capital initiatives will only succeed if they are subjected to rigorous and continuous analysis, evaluation, transparency, and learning. These efforts will build a workforce that fosters a shared commitment to U.S. national security and enhance its resilience.

GOAL 3

GOAL 3: Deliver Interoperable and Innovative Solutions at Scale

Promoting technical and tradecraft competitiveness and innovation for the Intelligence Community requires sustained investment and rapid adaptation of interoperable solutions at scale.

The Community will remove barriers by establishing unified IC procurement authorities, centralized solicitation systems, and a Community-wide contracting system, all bolstered by automation tools. A Community-wide, data-centric approach based on common standards is crucial to realizing the full promise of new capabilities. In response to changing mission needs, the IC will foster a culture that embraces innovation and the application of tools, data, processes, and standards necessary to transform labor- and time-intensive work into more efficient and productive human-machine partnerships. These efforts will include initiatives to improve the discoverability, accessibility, and standardization of our data.

The IC will also pursue complementary efforts to anticipate adversaries' over-the-horizon plans, capabilities, and intentions to inform Community research and development initiatives, guide capability development decisions, and avoid strategic surprise. The IC will also maximize the chances for technical breakthroughs and enhanced mission effectiveness by sustaining predictable funding for the research and development of new capabilities. This will require enhanced integration between the Community's science and technology enterprise and its collection and analysis communities to optimize resource allocation through coordinated investments.

The IC's emphasis on enterprise-wide solutions will benefit from expanded and diversified partnerships that the Community will leverage to develop and implement solutions that identify and anticipate capability gaps. These relationships will also allow the IC to harness state-of-the-art technology deliberately, lawfully, and ethically, in service of the Nation's security.

GOAL 4

GOAL 4: Diversify, Expand, and Strengthen Partnerships

Our unmatched network of alliances and partnerships around the world is our most important strategic asset—and a force multiplier for our intelligence mission. Our ability to leverage and work in concert with a broad set of partners enhances our operational capabilities, sharpens our insights, and strengthens the foundation for strategic relationships and common action between our governments.

That is why the Intelligence Community, like other members of the national security community, is committed to reaffirming, expanding, and enhancing our alliances and partnerships across regions and issues to meet the challenges and seize the opportunities of the future.

The IC has traditionally been organized and postured to understand the plans, intentions, and impacts of nation states and, following the 9/11 attacks, asymmetric threats from terrorist organizations. The series of interconnected and transnational threats facing the United States and its allies and partners requires a greater and more synchronized effort to enhance intelligence sharing across a broader swathe of issues and with a more diverse array of regional and local partners.

Even as we continue to invest in existing partnerships like those with our Five-Eyes partners and forge new ones, the evolving set of challenges—from cyberattacks and climate change to pandemics and foreign malign influence—also require investing in new and more diverse partnerships, especially with non-state and sub-national actors. From companies to cities to civil society organizations, these actors' ideas, innovations, resources, and actions increasingly shape our societal, technological, and economic futures.

The IC must rethink its approach to exchanging information and insights with non-state actors that either have the responsibility to act or are the entities best postured to do so in defense of U.S. national security interests. This is especially true of non-state actors positioned to detect and defend against cyber threats to critical infrastructure. The IC must adopt new approaches that take full advantage of non-state actor expertise and insights that are necessary for the Community to fulfill its mission. To these ends, the IC must build new and restructure existing collaborative mechanisms with non-state actors and find ways to enhance the flow of information to and from these actors in ways that safeguard our national security and prosperity.

GOAL 5

GOAL 5: Expand IC Capabilities and Expertise on Transnational Challenges

A highly connected and complex world means that transnational and transboundary challenges are having increasingly broad implications for U.S. interests in every region and in multiple domains. The world is facing more frequent and intense crises due to the effects of climate change, narcotics trafficking, financial crises, supply chain disruptions, corruption, new and recurring diseases, and emerging and disruptive technologies. Moreover, these cross-border challenges are increasingly interacting with and compounding traditional state-based political, economic, and security challenges with unexpected second consequences, from food and energy insecurity to irregular migration, and civil unrest to conflict.

The National Security Strategy makes it clear that these intensifying transnational challenges are at the core of national and international security. Accordingly, the IC is determined to improve its ability to understand, anticipate, and provide early warning about transnational threats, as well as identify opportunities for the United States, its allies, and partners. The IC will recruit, develop, and integrate expertise across a range of disciplines, such as climate and environmental security, global public health, biosecurity, science, and technology, to ensure it provides decision-makers actionable strategic foresight.

The IC must work across organizational boundaries and collaborate with other government agencies—both federal and local—to better integrate research, expertise, and data, and build the capacity to model and forecast potential cascading effects of these transnational challenges. The IC will build enduring partnerships with foreign partners, the private sector, academia, and others to leverage their unique capabilities and expertise and to augment its own ability to identify and prepare for challenges in both the near and long terms. The IC will leverage and enhance the tools, techniques, and procedures developed for other missions, such as counterterrorism, and apply lessons learned and best practices from these areas to evolving, transnational issues.

GOAL

GOAL 6: Enhance Resilience

The IC has an expanding role in supporting the resilience of the Nation, its allies, and its partners, particularly in a world still emerging from the COVID-19 pandemic. In this increasingly complex environment, risk assumed by one is effectively assumed by all, resulting in the need for a multifaceted, layered, and distributed approach that adapts as the threat evolves. Protecting the IC's and the Nation's critical infrastructure from complex threats requires a deeper understanding of the implications of destabilizing trends, and improved early warning to improve the Nation's recovery and response.

Resilience also includes defending the Nation's economic security and prosperity. That is why the IC is expanding its role in understanding threats and vulnerabilities to supply chains and helping to mitigate threats to government and industry partners' infrastructure. And it is why the Community will enhance transparency with federal, state, local, tribal, and territorial governments; non-state actors; and allies with a stake in the Nation's critical infrastructure. The Community will normalize information exchanges and research and development collaboration with governmental and non-state actors responsible for safeguarding critical infrastructure and systems that are vital to the Nation's prosperity.

The IC's resilience will be supported through modernization and hardening of its own infrastructure for adaptability, durability, redundancy, and interoperability. These efforts will ensure the Community has a continued ability to accomplish its mission and sustain its focus on the most important long-term threats in the face of inevitable crises such as pandemics, cyberattacks, climate shocks, and terrorist attacks. Equally important, the IC must sustain its counterintelligence capabilities and expertise against espionage and other damaging intelligence activities conducted by our foreign adversaries. Resilience will also involve safeguarding the IC workforce and upholding our sacred obligation to protect and care for officers and their families in harm's way.

Organization of the Intelligence Community

The Intelligence Community is an integrated enterprise comprised of 18 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 Director of National Intelligence (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 18 Elements:

TWO INDEPENDENT AGENCIES

1. The Office of the Director of National Intelligence (ODNI)
2. The Central Intelligence Agency (CIA)

NINE DEPARTMENT OF DEFENSE ELEMENTS

The following elements also receive guidance and oversight from the Under Secretary of Defense for Intelligence and Security (USD I&S)—

1. The Defense Intelligence Agency (DIA)
2. The National Security Agency (NSA)
3. The National Geospatial-Intelligence Agency (NGA)
4. The National Reconnaissance Office (NRO)
5. U.S. Air Force Intelligence
6. U.S. Navy Intelligence
7. U.S. Army Intelligence
8. U.S. Marine Corps Intelligence
9. U.S. Space Force Intelligence

SEVEN ELEMENTS OF OTHER DEPARTMENTS AND AGENCIES

1. The Department of Energy's Office of Intelligence and Counterintelligence
2. The Department of Homeland Security's Office of Intelligence and Analysis and
3. The intelligence and counterintelligence elements of the U.S. Coast Guard
4. The Department of Justice's Federal Bureau of Investigation and
5. The Drug Enforcement Administration's Office of National Security Intelligence
6. The Department of State's Bureau of Intelligence and Research
7. 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. Program managers are IC element heads responsible for the execution of their element's mission and budget. ODNI leads intelligence integration across these elements to deliver the most insightful intelligence and make the Nation more secure.


STATE
TREASURY
INDEPENDENT AGENCIES
JUSTICE
HOMELAND SECURITY
ENERGY
DEFENSE
UNITED STATES INTELLIGENCE COMMUNITY
COLLABORATUS
VIRTUS
FIDES


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA

UNITED STATES INTELLIGENCE COMMUNITY
INFORMATION
VIRTUE
FIDELITY