ODNI STRATEGY

2024

Twenty years ago, the Office of the Director of National Intelligence (ODNI) was created with the expectation that, as President Bush indicated at the time, "our vast intelligence enterprise will become more unified, coordinated, and effective." The first Director of National Intelligence (DNI), Director Negroponte, stated that our charge is clear:

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

Over the last two decades, we have worked to fulfill this vision. Significant strides have been made to promote a more unified, coordinated, and effective community—one that leverages each collection discipline to greater effect, as well as the deep expertise that resides across the Intelligence Community (IC) to produce and promote unified approaches to the most critical national security threats that our country faces. This work is evident in a variety of contexts, as policymakers and the warfighter often turn to ODNI to produce analytic products that provide IC-coordinated views on critical issues; evaluate the cost, schedule, and performance of major systems acquisitions, including through the production of independent cost estimates and projections; and develop strategies, policies, and standards that drive the IC toward common objectives.

We are, at the same time, executing against our mission in the context of an evolving national security environment, which is far more focused today on strategic competition, increasingly complex and intense transnational threats, and regional conflicts with global impact. Even so, twenty years later, our charge remains the same and our strategy is designed to ensure we maintain our focus.

Our evolution has been guided, in part, by ODNI's National Intelligence Managers and National Intelligence Officers, who are crucial in ensuring appropriate allocations of resources for collection and coordinated analysis across every functional and regional national security and foreign policy issue of relevance, consistently working to promote a strategic outlook for the

community as the threat landscape evolves. They have been instrumental in promoting integration and the alignment of IC resources to national priorities. ODNI has also, over time, worked to develop IC-wide policies that reduce duplication and enable greater interoperability to allow the sum of our community to be greater than its parts. Over the past few years ODNI has, in particular, played an increasingly prominent role in leveraging IC-wide expertise and resources to make progress on emerging issues as diverse as Artificial Intelligence (AI), microelectronics, biosecurity, and economic security to great effect.

There is more progress, however, to be made. ODNI is instituting a range of new initiatives designed to develop structures, mechanisms, and processes to further promote collaboration across the IC and beyond, leveraging each element's strengths to the benefit of all and enhancing resilience. This encompasses efforts to build and nourish ties with partners and allies of various types around the world on issues both tactical and strategic, both in the United States and abroad. The IC's intelligence diplomacy is one such initiative, as is our effort to revolutionize our partnerships with the private sector and academia. But this also includes our work to promote a data-ready IC, to promote innovation that can be scaled across the IC, to develop an IC information technology architecture that will support our work in the decades to come, to better leverage open source intelligence, and perhaps most importantly, to build trust and confidence with the IC workforce, the Congress, and the public.

Finally, understanding that our people are our greatest asset, ODNI is working to ensure we are recruiting, developing, and retaining the diverse and talented IC workforce needed to face the future, building a culture that promotes respect and dignity, strengthening our resilience with IC institutions that are capable of being agile, promoting the integrated expertise that is needed to address a broader definition of national security, and facilitating the partnerships—both in and out of government—that are crucial to our success.

Goal 1

Aligning our National Intelligence Resources to our National Priorities

By statute, ODNI develops and ensures the effective execution of an annual budget for the IC, which is known as the National Intelligence Program. Our foremost responsibility is to steward the IC's investments in alignment with national priorities and in pursuit of the goals articulated in the National Intelligence Strategy (NIS). This means remaining focused on the concerns identified in the President's National Security Strategy, the National Defense Strategy, and the Annual Threat Assessment. All of these documents highlight an accelerating strategic competition with major authoritarian powers and some regional powers; intensifying transnational threats; and more capable non-state actors that are challenging longstanding rules of the international system. The IC must cover these, even as we meet the demands of multiple crises and surges, such as Russia's invasion of Ukraine and the war in Gaza.

ODNI also works to ensure that the IC's efforts are aligned to the national priorities through organizational structures and processes. For example, in the context of transnational threats, we have preserved the National Counterterrorism Center (NCTC) and its efforts to protect our Homeland against terrorism—honoring a foundational responsibility to the American people. ODNI has also applied lessons learned in the context of counterterrorism to counternarcotics, a crucial national security priority to enhance our focus and integration across the IC in this mission area. Specifically, we established the IC Counternarcotics Executive, which capitalizes on NCTC's expertise, processes, and tools to bring cohesion within the IC in support of policymakers and law enforcement officers who are confronting the scourge of synthetic opioids in the United States.

In the end, all of these efforts are reflected to decision-makers through an increasingly essential and externally engaged National Intelligence Council and an ever-vital President's Daily Brief, designed to provide the IC's tactical and strategic analyses to our senior-most leaders regarding the most complex policy challenges we face today. These products and services are our calling card and we proudly claim them, knowing that we rigorously adhere to the highest standards of tradecraft to convey what we know, what we do not know, and when there are competing views within our community.

Effective stewardship of our resources is critical to supporting the intelligence and analysis that gives our decision-makers an advantage and often means making hard but informed choices about what we protect and promote and where we take risk, while learning how to better leverage each other's investments across the IC and making long-term investments that better position our community for strategic competition in a complex and often short-term budget environment. ODNI is—through mission analytics—bringing integrated data-driven resource decisions closer to reality, digging deeper than the surface-level reflections of dollars invested and measurable outcomes produced by examining how well the IC responds to customer priorities, the quality and relevance of our insights, and which capabilities offer the best return on investment to address gaps.

Goal 2

Promoting Expertise, Data, Science, and Innovation

ODNI will continue developing a digitally savvy workforce with deep technical, data, and scientific expertise. In an increasingly complex, interconnected, and evolving threat environment, ODNI and IC mission success depends on the knowledge and skill of our workforce to adapt to a reality shaped by massive amounts of data, leveraging industry-leading technology to discover threats and derive novel insights. We must furthermore improve the efficiency and effectiveness of our capacity to identify, develop, acquire, and scale innovation produced in and out of government, including by leveraging the expertise resident in federal agencies, academia, and industry.

Both the 2023–2025 IC Data Strategy and recently issued IC Directive 504 prioritize data as a strategic and operational asset and establish a path toward a data-ready IC capable of meeting the threats of today and tomorrow. End-to-end data management planning, data governance, and federal computational standardization are fundamental to data interoperability, which will unlock the potential inherent in scaling advanced analytics and human-machine teaming, as well as the use of AI, quantum, and other emerging technologies at mission speed. Data centricity with robust data governance will ultimately lead to real-time, accurate, and appropriate data sharing for impact across the IC; the federal government more generally, as well as state, local, tribal, and territorial partners; the private sector; and international partners.

And just as the IC Data strategy prioritizes data as a resource, multiple IC strategies prioritize innovation as a mindset to be embraced and enabled by ODNI across the IC. We realize that in order to meet the challenges of the modern world, advances in adversaries' capabilities, and an era of global strategic technology competition, it is imperative that we become more agile in adopting and scaling innovative technologies to meet mission needs and consequently we are investing in a series of efforts that we believe will help us do just that.

To achieve greater speed in scaling the right technologies and tools, ODNI will continued to develop and issue acquisition guidance that incorporates best practices to assist IC elements in strengthening their relationships with entities involved in cutting edge technology, including through increased SCIF access; promoting innovation hubs that enable industry, academia, and the IC to come together to create, collaborate on, and innovate game-changing technologies to serve our mission; holding training sessions to help IC elements leverage the recently delegated Other Transaction Authority that Congress passed; working with industry to develop an emerging technology curriculum that will familiarize the acquisition workforce with the unique business considerations of emerging technology companies and the full spectrum of acquisition authorities to integrate and scale innovative technologies; supporting models that better integrate the program manager, mission, and technical leads through the acquisition adoption cycle to accelerate user adoption and innovation at the speed of mission; and exploring novel contracting approaches, such as IC-wide contract vehicles that increase acquisition agility and make it easier to scale innovation successfully adopted by one element, across the IC.

While so much of what has already been identified as part of this second goal is related to AI, it is worth calling out the changes driven by the proliferation of AI, particularly generative AI, and the importance we attach to integrating AI into IC processes and workflows at scale. The IC will increasingly leverage AI to provide efficiencies and new insights in the production of analysis, declassification, automation of repetitive tasks, and in so many other ways to ensure we are taking advantage of the opportunities offered by these developments, even as we focus on countering malicious uses of AI, on understanding the broader implications of AI-related developments on national security, and on how to ensure that our uses are governed by the law, our values, principles, and ethics in all circumstances.

Goal 3

Enhancing IC Partnerships

In today's strategic environment, the IC must embrace new partnerships and external perspectives to be effective. This isn't just about sharing information, though that is part of it—we need to understand each other better, learn from each other, work together more closely, grow together, protect each other, and sometimes even make decisions together. Increasingly, informed judgments reside with not just state actors but also non-state entities (NSEs), from companies to academia to cities to civil society organizations. With this in mind, ODNI's IC-wide NSE initiative spawned a suite of changes that will revolutionize public-private, sub-federal, and transnational partnerships for the IC, thereby expanding our sources of insights, promoting our capacity to scale innovation across the IC, and our ability to protect our private sector. To cement our work in this arena, we have established an Office of Partner Engagement within ODNI to facilitate the IC's partnership efforts and to evaluate our success.

At the same time, ODNI is promoting an architecture that supports strengthened multilateral intelligence networks in support of our national security and foreign policy objectives. Intelligence diplomacy, which we see as a strategic tool, proved its value to our alliance efforts in the context of Russia's brutal and unprovoked invasion of Ukraine in February 2022, and is now understood to be an indispensable method for developing a common threat picture with coalitions of allies and partners capable of driving action in favor of mutual policy and security objectives while also expanding and deepening our partnerships. These efforts are intended to be wide ranging, and are intended not simply to enhance our liaison partnerships, but help provide a common and trusted analytic and reporting baseline in support of policy efforts to manage shared threats. ODNI leadership will be essential to ensuring that these changes are integrated and sustained throughout the IC.

The combined impact of enhancing these different types of partnerships is another dimension of the challenge and the opportunity we are seeking to seize. For example, in several areas, our efforts to enhance both NSE partnerships and multilateral relationships are mutually reinforcing and together produce greater impact than either could alone, most notably in the context of emerging technologies. The formation of the Office of Economic Security and Emerging Technologies (OESET) to lead the IC's shift toward addressing techno-economic competition reflects more than a new mission—it is a new way of achieving our mission—and underscores the view that economic security is national security. OESET is leveraging state partner financial intelligence while also leveraging NSE partners outside of government for foundational analysis that will enhance and expand IC support to policymakers, redefining how data is accessed, developing a new supply chain analytic discipline, and strengthening partnerships across government on emerging technology and economic statecraft.

ODNI is also expanding and strengthening the mechanisms through which external expertise can be accessed and developed to produce unique insights. For example, we have re-energized the Cyber Threat Intelligence Integration Center (CTIIC), which is now driving innovation and convening industry-analytic exchanges that bring together the IC and other government partners, critical infrastructure owners and operators, industry associations, as well as industrial control systems and cybersecurity industries for focused discussions that provide new insights. These engagements, along with CTIIC's IC-enterprise acquisitions of commercial cyber-threat intelligence, are improving the IC's ability to warn of foreign cyber threats and deliver actionable analysis to the policy and critical infrastructure communities. ODNI also established an IC Climate Lab that fuses climate science expertise at the National Labs with intelligence, improving the IC's ability to anticipate environmental impacts on a range of national security interests. In addition, ODNI's National Intelligence University (NIU) recently established a research lab where students, government employees, and experts from industry and academia are attempting to address some of the nation's most pressing technological challenges.

ODNI is also expanding and strengthening our collaboration with the private sector and academia to assist those who are under attack from foreign intelligence and security services through improved information sharing, analytic insights, and collaborative threat mitigation efforts. ODNI's National Counterintelligence and Security Center (NCSC) is the primary organization within the U.S. Government for managing, coordinating, and integrating counterintelligence activities. NCSC is in the process of establishing a pilot Joint Threat Assessment Team (JTAT) that draws on the Joint Counterterrorism Assessment Team model, which was established with great effect at NCTC years ago to improve information sharing and enhance public safety. This new pilot will similarly be focused on improving information sharing with key private sector and academic, research, and scientific institutions that are subject to intelligence and security threats. In coordination with the Federal Bureau of Investigation and the Department of Homeland Security, the JTAT will collaborate with other members of the IC to research, produce, and disseminate intelligence and security threat information for private sector entities within prioritized technological sectors, and advocate for the intelligence requirements and needs of these institutions.

Goal 4

Strengthening Resilience

The NIS highlights the IC's critical and expanding role in supporting the resilience of the Nation, its allies, and its partners. The IC's own resilience will also be supported through modernization and hardening of its own infrastructure and capabilities for adaptability, durability, redundancy, and interoperability. These efforts will ensure the IC has the ability to accomplish its mission and sustain its focus on the most important long-term threats even as we continue to manage the demands of urgent crises and surges. Equally important, the IC must sustain its counterintelligence capabilities and expertise against espionage and other damaging intelligence activities conducted by our foreign adversaries. Resilience involves safeguarding the IC workforce and upholding our sacred obligation to protect and care for officers and their families. The following examples highlight approaches the IC is taking to increase its resilience in four key areas.

Space capabilities are vital to the U.S. economy and national security, and have long been a critical part of the IC's collection architecture. But over the last two decades, Russia and the People's Republic of China have increasingly pursued counterspace weapons capable of targeting U.S. and allied satellites. ODNI is generating a space resiliency strategy that accounts for scenarios across competition, crisis, and conflict to rationalize and prioritize critical resilience efforts and investments. The IC has, in an effort to protect our space mission capabilities, made significant strides in improving redundancy, protection against cyber threats, and development of robust on-orbit capabilities to operate in the increased threat environment. This has included the development of proliferated, resilient constellations with the Department of Defense, and leveraging commercial satellite and launch capabilities.

The IC is doing similar work with respect to the IC's information technology (IT) infrastructure, which is not only foundational to our resilience, but also will continue to grow exponentially as we further leverage AI in support of our mission. ODNI must oversee and ensure that the IC's IT infrastructure is not only secure and highly resistant to various potential disruptions such as global unrest, terrorist attacks, cyberattacks, and natural disasters—but also that our IT infrastructure is capable of automated "self-healing" and scalable to support unpredictable demands. After all, we must reliably enable the intelligence mission anywhere, including empowering the edge and providing resilient IT capabilities in disconnected, denied, intermittent, and limited bandwidth environments. We employ a zero-trust security model to alleviate cybersecurity threats and vulnerabilities, and deploy safeguards against adversarial quantum capabilities. A resilient, reliable, and secure IC IT infrastructure has the capacity to reduce operational downtime and the impact of operational threats, while simultaneously increasing data protections and allowing us to maintain a competitive advantage over our adversaries. To achieve these outcomes, the Office of the IC Chief Information Officer has established the Vision for the IC Information Environment: An Information Technology Roadmap. This Community-developed and endorsed document will enable the IC to make strategic and substantive IT investments in support of a resilient architecture underpinning our intelligence mission.

Another key area that we are focused on in support of our Nation's resilience is foreign malign influence efforts, including election threats, as defending against such threats is critical to protecting our democracy. As part of this effort, the Foreign Malign Influence Center (FMIC) works closely with the interagency to share relevant and actionable intelligence with federal, state, and local partners in a timely manner; conducts exchanges with technology companies on evolving foreign adversary tactics, techniques, and procedures, as well as authentication and attribution methodologies; and engages foreign liaison and civil society experts to learn from their experiences. We are also publishing regular updates to keep the American public informed about the efforts being undertaken by foreign countries to attempt to undermine the integrity of U.S. elections and drive wedges in U.S. society. To ensure knowledge capture and guard against brain drain between election cycles, FMIC is developing a new unified intelligence strategy dedicated to foreign malign influence; has produced updated collection emphasis memos to highlight the challenge posed by AI; and has implemented standard operating procedures to enhance our capability to warn against foreign election-related influence efforts and conduct media authentication to identify, for example, deep fakes.

Every area in which we work to promote resilience is entirely reliant, of course, on the health and well-being of our workforce; people who are assigned to do some of the most stressful and challenging jobs available. ODNI is committed to supporting them, including by offering workplace flexibilities and other workforce resources to balance mission and personal needs.

Goal 5

Building Trust and Confidence

Building trust and confidence with the IC workforce, the Congress, and the public is necessary to protect the American people and to do so, we must uphold our democratic values and ensure that we are living in compliance with the law, our principles, and the ethos they represent.

We have articulated our core ethical principles in the Principles of Professional Ethics for the Intelligence Community: mission, truth, lawfulness, integrity, stewardship, excellence, and diversity. We seek to live in accordance with these principles and to build trust by pursuing initiatives that facilitate transparency, oversight, and a diverse workforce culture that promotes respect and dignity, where people feel supported for who they are, able to raise concerns and share ideas, and ultimately empowered.

ODNI's transparency initiatives seek to release material on matters of public interest, to help people understand what we do, to promote trust and credibility, to inform our citizenry on matters of national security, and to promote accountability. We have launched a proactive transparency program to facilitate such work, we will continue to seek opportunities to release information about the frameworks that govern IC activities and IC decision-making to the greatest extent possible, and the NIC will continue to expand its public release of unclassified and declassified analytic and outreach products on emerging global issues. Furthermore, ODNI will continue to publish material on intel.gov. and dni.gov to provide the public a clearer window into our work—or as Director Clapper said: "to correct misunderstandings and to try to help people grasp what we do, to show that we're worthy of America's trust, and to prove that we make worthwhile contributions to the security of Americans and our friends and allies around the world."

Not unrelatedly, ODNI is also driving classification reform. ODNI is working on implementing a series of initiatives to address systemic challenges related to over classification. Among these initiatives are commitments to reduce ODNI's Freedom of Information Act (FOIA) backlog and timelines to meet declassification obligations, including through the use of new technologies.

Of course, central to our work on building trust and confidence internally and externally is a fundamental commitment to civil liberties and privacy. Our Chief Civil Liberties, Privacy, and Transparency (CLPT) Officer is an independent adviser to the DNI who ensures that the IC's missions, programs, activities, policies, and technologies protect privacy and civil liberties. Our CLPT Officer works to ensure that as we leverage our capabilities and new technologies to face evolving threats and adversaries, we are guided by ethical, inclusive, and equitable frameworks and policies that protect privacy and civil liberties—and that, to the greatest extent possible, we make public those policies and frameworks. For example, in the spring of 2024, we proactively released our policy framework governing the IC's access to, collection, and processing of commercially available information.

Goal 6

Strengthening our Institution and our Workforce

The IC's workforce is our most precious asset and our future success depends on our ability to continue to attract and retain a highly talented workforce that draws on one of our country's unmatched reservoirs of strength: our diversity. If we are to succeed, it is imperative that we hire and retain talent from a wide variety of backgrounds and experiences that reflect the extraordinary diversity in our country, allowing us to tap into the talent that resides in our nation to keep our country safe.

To accomplish this, ODNI is pursuing technology and process enhancements to modernize recruitment, hiring, and vetting processes. ODNI has developed a flexible approach to career pathing that supports the need for expertise in critical mission areas, fosters workforce mobility, and enables succession planning. In conjunction with this approach, ODNI has offices, geared toward, among other things, addressing concerns about the hiring and vetting process. ODNI is also investing in mentoring and coaching programs that meet the needs of its joint workforce of permanent cadre and detailee officers from other IC agencies. These efforts—combined with ODNI's commitment to a promotion process that is equitable, transparent, and consistent with mission requirements—will enable us to recruit, retain, develop, and recognize talent while we continue to build the next generation of IC leaders.

ODNI will continue to evaluate and streamline internal business processes with a focus on promoting agency-wide acumen and ownership of financial and resource management processes, including ODNI's use of contracts to support its mission. ODNI recognizes that the ability to quickly and effectively respond to emerging threats requires flexibility and agility to pivot to address new challenges. To address this, we will continue to build upon our progress in meeting the 180-day hiring goal and to adopting business process and employee resource innovations that foster an adaptable and resilient workforce.

Concurrently, ODNI will support and promote the use of shared IC hiring and recruiting platforms, virtual tool suites, and advanced analytics to improve candidate access and IC-wide onboarding timelines, as well as recruiter targeting, resource management, communication, and decision-making. We will continue to promote IC-wide diversity, equity, inclusion, and accessibility using a data-driven approach to identify and address the IC's diversity gaps and personnel challenges by collecting and analyzing workforce demographic data, strengthening strategic partnerships, delivering evidence-based training, and incorporating best practices.

Finally, we will consistently support the development of our workforce and among our greatest assets in doing so is the National Intelligence University, which is the IC's accredited, federal degree-granting institution. NIU enriches our work and is charged with preparing the next generation of leaders of the IC to meet the future.


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA