OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PUBLIC AFFAIRS OFFICE
WASHINGTON, D.C.
20511

Fact Sheet: Real Progress in Reforming Intelligence

The Intelligence Reform and Terrorism Prevention Act of 2004 did more than create the Office of the Director of National Intelligence – it charged the Office with significantly reforming and strengthening America's Intelligence Community. Under the leadership of Director John D. Negroponte, the ODNI has revitalized, reformed, and led the Community to better protect our nation by:

Ensuring that we collect the right intelligence in the best ways to most accurately and objectively guide national intelligence.

- Strengthened the connection between collection and analysis by appointing Mission Managers for key hard target issue areas and enduring intelligence challenges. The North Korea and Iran Mission Managers have already begun promoting Community-wide integration and providing policymakers with briefings drawing on Community-wide expertise.

- Initiated an Integrated Collection Architecture process to develop an objective architecture and implementation roadmap that looks at various collection disciplines in an integrated fashion.

- Worked closely with the Department of Justice and the Federal Bureau of Investigation to establish the FBI's National Security Branch to integrate the FBI's counterterrorism, counterintelligence, and intelligence programs.

- Facilitated the establishment of a National Clandestine Service at CIA with the Director of CIA serving as the National HUMINT Manager.

- Created the MASINT Community Executive to provide this important intelligence discipline with a voice at the table, an advocate in budget and policy decisions, and the impetus for further advancement.

Focusing and strengthening our analytic work, better ensuring that our policymakers receive the highest-quality analysis to guide their decisions.

- Streamlined production of National Intelligence Council (NIC) products, increasing output and minimizing delays in production time, and implemented more effective explanation of the reasoning behind judgments and the portrayal of alternative views of analysts.

- Created a Long-Range Analysis Unit within the NIC made up of eleven analysts, including the six recipients of the annual DNI Exceptional Analyst Fellowship and two outside nongovernmental experts.

- Acquired new and important items for the PDB reflecting the unique strengths of the full Intelligence Community and enhanced strategic planning for the PDB, to better tap expertise within the Community, better support the policymaking process, and provide advance warning of issues of concern on the medium to long term horizon.

- Disseminated the first IC Analytic Standards, capturing the best practices from across the Community, the lessons learned from the past, and the goals of reform.

Providing a clear direction to guarantee timely and meaningful results.

- Promulgated the first unclassified *National Intelligence Strategy* (NIS), linking the Community's goals to the National Security Strategy and establishing specific objectives and metrics for accomplishment. Also began implementation of a structured strategic planning process to ensure NIS objectives are met.

Directly answering the specific needs of our intelligence customers.

- The DNI created the Requirements Directorate to give the IC's diverse customers a responsive mechanism with which to articulate their intelligence needs, determine the extent to which the IC is addressing those needs, and facilitating a process to make changes if it falls short of those needs.

- Created the Foreign Relations Coordinating Committee to synchronize Intelligence Community foreign outreach efforts and maximize opportunities for the U.S. to achieve intelligence goals and national policy objectives. For example, a new intelligence relationship was expeditiously established with a country and an existing relationship with another country is being enhanced as a Community effort instead of the traditional "stove-piped" approach to partner relationships.

- The Requirements Directorate's Homeland Security and Law Enforcement Office is creating partnerships between domestic law enforcement and intelligence organizations and building the framework whereby information that affects our homeland security can be shared in a timely manner, consistent with our responsibility to respect the rights of our citizens.

- DNI undertook a major after action review of IC performance during recent activity by North Korea to test ballistic missiles and a nuclear device. The Requirements Directorate's Military Support Office reached out to 29 organizations – IC components and IC customers – with the goal of assessing IC-level processes to support policy makers and military commanders. The review provided six key lessons learned, and 23 specific process recommendations for the DNI to consider. In the process, key IC leaders like the North Korean Mission Manager refined roles and responsibilities, improving the ability of the DNI to fulfill the spirit and intent of The Reform Act and National Intelligence Strategy.

Dismantling the "stovepipe" mentality that said agencies could produce, and limit within its walls, vital national intelligence.

- The National Counterterrorism Center (NCTC) is drawing on collected terrorist intelligence from agencies across the U.S. Government – with access to more than 30 different networks – to produce integrated analysis on terrorist plots against U.S. interests at home and abroad. This is being done nowhere else in government – and it was only an aspiration prior to 9/11.

- NCTC is working closely with liaison partners to broaden our information sharing capabilities. During the past year, NCTC shared hundreds of analytic products with foreign partners, and in return, we received hundreds of terrorism-related products from them. In the same period, NCTC has also hosted approximately 200 meetings with foreign counterterrorism officials and organizations.

- The National Counterproliferation Center (NCPC), the mission manager for counterproliferation, in conjunction with its Intelligence Community and ODNI partners, has developed integrated and creative strategies against some of the nation's highest priority targets—to include "Gap Attacks" (focused strategies against longstanding intelligence gaps), "over the horizon" studies to address potential future counterproliferation threats, and specialized projects on priority issues such as the Counterterrorism-Counterproliferation Nexus.

- Developed and advanced an interagency approach to strategic interdiction, as recommended by the WMD Commission.

Moving the Intelligence Community forward to adopt a Community-wide technology architecture.

- The Chief Information Officer (CIO), appointed in December 2005, implemented a classified information sharing initiative that enhanced and expanded information sharing with key U.S. allies. While the success of this program is only one step toward overhauling the IC's information management system, it represented a paradigm shift in the Community's information sharing policies.

- The CIO also established the Unified Cross Domain Management office with DoD to oversee development and implementation of common technologies that enable highly classified networks to share information with users and systems that have lower or no clearances.

- The CIO overcame barriers to information sharing and implementation of information sharing standards. For example, by dismantling prohibitive firewalls, leveraging commercial technologies, and inter-connecting DoD and IC transport systems, the CIO allowed for broader federal access to INTELINK's Sensitive But Unclassified domain.

Working to share intelligence with affected parties *outside* the Intelligence Community.

- Created a Program Manager for the Information Sharing Environment, who recently released the Information Sharing Environment Implementation Plan and Privacy Guidelines which provides the vision and road map for better sharing information within the Intelligence Community and with our fellow Federal, State, local, and tribal counterparts, as well as with the private sector.

Making significant investments in building a strong IC workforce.

- The ODNI has developed a comprehensive IC-wide human capital plan and is establishing "joint duty" as a requirement for promotion to senior positions.

- The DNI has appointed a Chief of Equal Employment Opportunity and Diversity for the IC (EEOD). The DNI has agreed in principle to a wide-ranging set of recommendations that the Diversity Senior Advisory Panel for the IC (DSAPIC) made in their report: *Diversity: A National Security Imperative for the Intelligence* Community.

Leading the way with the latest technologies.

- For the first time ever, the Intelligence Community's Science and Technology (S&T) leadership created a joint S&T plan that identified major unmet needs for the IC as a whole as well as opportunities for broader cooperation to satisfy those needs.

- As part of the overarching plan, S&T initiated several joint programs that target the community's most pressing problems and forge cross-community teams in the process. Some of these teams have already delivered prototypes of innovative new technologies to combat terrorism. S&T is also preparing an ambitious plan to accelerate the deployment and cut the cost of major capabilities that will benefit multiple agencies.

- S&T has implemented the Rapid Technology Transition Initiative, a program that identifies low cost, high value technologies that the ODNI can put in the hands of users quickly. Congress provided the first year of pilot funding for the effort, and S&T will soon be awarding the top 13 candidate projects. All will be delivered in approximately six months for direct use in the Global War on Terrorism.

Always being mindful that our actions must befit the highest traditions of civil liberty and privacy protection.

- Appointed a Civil Liberties Protection Officer and staffed an office to ensure that the policies of the IC incorporate protections for privacy and civil liberties, to oversee compliance by the ODNI with legal requirements regarding privacy and civil liberties, and to ensure that the use of technology sustains, and does not erode, privacy.

# # #