Senate Homeland Security and Governmental Affairs Committee

10 September 2007 hearing on

Confronting the Terrorist Threat to the Homeland: Six Years after 9/11

Statement for the Record

of

J. Michael McConnell

Director of National Intelligence

Statement for the Record

Director of National Intelligence, 10 September 2007
Senate Committee on Homeland Security and Government Affairs
"Confronting the Terrorist Threat to the Homeland: Six Years After 9/11"

Chairman Lieberman, Ranking Member Collins, and members of the Senate Committee on Homeland Security and Government Affairs: Thank you for your invitation to appear before the committee to provide a status report on the nation's efforts to confront terrorist threats to the nation and to describe the implementation of institutional reforms mandated by Congress and by Presidential directive since September 11, 2001.

It is my privilege to be accompanied by Michael Chertoff, Secretary of Homeland Security, Robert Mueller, Director of the Federal Bureau of Investigation, and Vice Admiral John Scott Redd, Director of the National Counterterrorism Center.

Terrorist Threat to the U.S. Homeland

I would like to begin my statement with a discussion of the findings of the July 2007 National Intelligence Estimate (NIE) on the Terrorist Threat to the U.S. Homeland. An NIE is the most authoritative written judgment of the Intelligence Community (IC) on a particular subject and a declassified version of this NIE's key judgments was made available on the Internet. It assessed the following:

- The US Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa'ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.
- Greatly increased worldwide counterterrorism efforts over the past five years have constrained the ability of al-Qa'ida to attack the US Homeland again and have led terrorist groups to perceive the Homeland as a harder target to strike than on 9/11.
- We are concerned, however, that this level of international cooperation may wane as 9/11 becomes a more distant memory and perceptions of the threat diverge.

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities. We assess the group has protected or regenerated key elements of its Homeland attack capability, including: a safehaven in the Pakistan Federally Administered Tribal Areas (FATA), operational lieutenants, and its top leadership. Although we have discovered only a handful of individuals in the United States with ties to al-Qa'ida senior leadership since 9/11, we judge that al-Qa'ida will intensify its efforts to put operatives here.
- As a result, we judge that the United States currently is in a heightened threat environment.
- We assess that al-Qa'ida will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. Of note, we assess that al-Qa'ida will probably seek to leverage the contacts and capabilities of al-Qa'ida in Iraq.
- We assess that al-Qa'ida's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the US population.
- We assess that al-Qa'ida will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.
- We assess Lebanese Hizballah, which has conducted anti-US attacks outside the United States in the past, may be more likely to consider attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.
- We assess that the spread of radical—especially Salafi—Internet sites, increasingly aggressive anti-US rhetoric and actions, and the growing number of radical, self-generating cells in Western countries indicate that the radical and violent segment of the West's Muslim population is expanding, including in the United States.
- We assess that other, non-Muslim terrorist groups probably will conduct attacks over the next three years given their violent histories, but we assess this violence is likely to be on a small scale.
- We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect

with one another, justify and intensify their anger, and mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.

The analytic effort that culminated in this NIE was strengthened by many of the intelligence reforms realized since September 11.

Intelligence Reforms Since 9/11

I turn now to the transformation we have undertaken in the IC to meet the challenges of today and the threats of tomorrow.

The Intelligence Community has made significant strides in addressing the underlying deficiencies exposed by the attacks of 9/11. This morning, I would like to first highlight a few of the flaws in America's intelligence system that existed before 9/11; second, detail the steps we have taken thus far to build a stronger Community; and, finally, turn our gaze to initiatives that will further these reforms.

Generally speaking, before 9/11 America's Intelligence Community was structured to win the Cold War—a traditional struggle between two great powers. The Community was downsized during the 1990s and while it consisted of over a dozen agencies with unique mandates and competencies, we lacked a national-level intelligence apparatus to manage effectively the Community and synthesize information from across the government to support a host of customers—policymakers, warfighters, and law enforcement officials—with various, and often competing, requirements. This construct led often to the "stovepiping" of information within agencies that guarded their cultures and their secrets. Data was provided on a "need to know" basis. "Information sharing" was considered more an exposure to foreign espionage than a path to a smarter intelligence enterprise. Accordingly, analysts in one agency were not encouraged to work with analysts in others. There were few processes in place to collaborate, share lessons learned and best practices, and manage the Community as an enterprise.

In the past, policy barriers also prevented the government from attracting young people of promise with the skills and backgrounds needed to strengthen our national defense. Too often, agencies became so focused on protecting sources and methods that they made it nearly impossible for first- and second-generation Americans to serve the intelligence enterprise. This was a serious deficiency that denied the country the efforts of those with the language fluencies, political, scientific, and technical skills, and cultural insights that we need to bolster our workforce and improve our intelligence.

Structurally, the Community was also largely divided between domestic and foreign intelligence.

The end of the Cold War and the advance of globalization enabled the acceleration of threats stemming from international terrorism, weapons of mass destruction (WMD) proliferation, failed states, and illegal drug trafficking. These threats, among others, move at increasing speeds due to technology and across geographic and organizational boundaries, blurring the distinction between foreign and domestic, and between strategic and tactical events. As we witnessed on 9/11, radical extremist movements continue to use global terrorism to further their causes by attacking innocent people without regard to national boundaries and state and non-state actors continue to demonstrate their intent to acquire WMD through illicit means.

To confront today's threats, we have made many changes in the way we conduct intelligence, law enforcement, homeland security, diplomatic, and defense activities. Implementing the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) along with the recommendations from various in-depth studies—such as the 9/11 Commission Report, the WMD Commission Report, internal Executive Branch reviews and reports by both houses of Congress—the Community received direction and the mandate and many of the tools needed to build an effective, results-oriented enterprise. The Intelligence Reform Act provided a mechanism for overhauling the IC by providing a new office, the Office of the Director of National Intelligence (ODNI), with the tools and mandate to unify and direct the efforts of our 16 intelligence agencies.

With these new mechanisms, we are working to forge an integrated Intelligence Community that spans the historical divide between foreign and domestic intelligence efforts. Far from being a buzz word, integration means ensuring that our various specialized intelligence missions operate as a single enterprise. An integrated and collaborative Community is a critical advance because no single agency has the capacity to evaluate all available information—lest we forget that over one billion pieces of data are collected by America's intelligence agencies everyday.

While we recognize that much more must be accomplished, the professionals of the Intelligence Community take pride in the notable progress we have made over the past six years. I would like to describe our accomplishments thus far in four main areas: our efforts to **structure** the Intelligence Community to meet 21st century challenges; **improve** analysis through cross-agency integration and technical initiatives; develop a **collaborative** Community that provides the right information to the right people at the right time; and **build** a dynamic intelligence enterprise that promotes diversity to gain and sustain a competitive advantage against our adversaries.

Structuring the IC

The principal legacy of the IRTPA was the establishment of the office of the Director of National Intelligence with assigned responsibilities to serve as the chief intelligence advisor to the President and National and Homeland Security Councils and to head the IC to ensure closer coordination and integration. The DNI is afforded responsibility to determine the National Intelligence Program and significant authority over personnel policy. In a larger sense, the creation of the DNI allows one person to see across the wide American Intelligence Community, identify gaps, and promote a strategic, unified vision.

I will leave to my colleagues with me here today the discussion of the specifics of their efforts, but I would like to highlight the key structural changes, in addition to the establishment of the ODNI, that have been undertaken since 9/11.

Working closely with the Department of Justice and the FBI, we supported the creation of the FBI's National Security Branch to integrate the FBI's counterterrorism, counterintelligence, WMD, and intelligence programs. We also supported the creation of Field Intelligence Groups in every FBI field office—a major steps in the FBI's effort to transform itself into a preeminent domestic counterterrorism agency. Furthermore, the Executive Assistant Director of the National Security Branch now works closely with me and my leadership team, ensuring close coordination on addressing the FBI's intelligence mission.

We established the National Counterterrorism Center (NCTC), the government's hub for all strategic level counterterrorism intelligence assessments, which draws on collected terrorist intelligence from agencies across the U.S. Government with access to more than 30 different networks carrying more than 80 unique data sources to produce integrated analysis on terrorist plots against U.S. interests at home and abroad. This kind of fusion is conducted nowhere else in government—and it was only an aspiration prior to 9/11.

The results are tangible. NCTC produces a daily threat matrix and situation reports that are the Community standard for current intelligence awareness. In addition, NCTC hosts three video teleconferences daily to discuss the threat matrix and situation reports to ensure the intelligence agencies and organizations see all urgent counterterrorism information.

We also established the National Counterproliferation Center (NCPC), the mission manager for counterproliferation, which has developed integrated and creative strategies against some of the nation's highest priority targets, including "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.

ODNI Mission Managers for high-priority topics, such as North Korea, Iran, counterintelligence, and Cuba and Venezuela, have also made considerable progress by identifying intelligence priorities, gaps, and requirements and engaging in strategic planning and collection management in the larger context of other intelligence collection and analytical priorities.

In the last few months, we also established an Executive Committee (EXCOM) to advise the DNI in the discharge of his responsibility for the coordination of all intelligence activities that constitute the domestic and foreign intelligence efforts of the country. This EXCOM is composed of the heads of all major intelligence producers and consumers and provides a biweekly forum for the key stakeholders to gather and provide common guidance on the development, implementation, and evaluation of activities of the IC.

Within the past six months, we also named a Deputy Director of National Intelligence (DDNI) for Acquisition to enhance the efficiency and effectiveness of our acquisitions. The DDNI for Acquisition has drafted a strategy to improve the acquisition process and recommended modifications to acquisition authorities. We are also in the process of standing up the Intelligence Advanced Research Projects Activity to create synergy and innovation across the IC by harnessing technology in new ways to create strategic advantage.

These three initiatives were highlighted by the Intelligence Community's 100 Day Plan for Integration and Collaboration, which we launched in April and concluded in August. The 100 Day Plan identified 24 specific initiatives and tasks to be accomplished on a rigorous timeline; of those 24, 17 tasks were achieved in that timeframe and the remaining tasks are scheduled to be met in the coming weeks. The Plan was designed to build on the successes so far—many of which I will discuss here—and to jumpstart further efforts. Initiatives were aligned to six integration and transformation focus areas:

1. Create a Culture of Collaboration
2. Foster Collection and Analytic Transformation
3. Build Acquisition Excellence and Technology Leadership
4. Modernize Business Practices
5. Accelerate Information Sharing
6. Clarify and Align DNI's Authorities.

I have discussed the specifics of this Plan in other forums and will not detail it today, although I note that the focus on accountability and achieving identified targets has given a renewed emphasis to transforming the Community and executing these reform initiatives. I will speak again of our planning process at the conclusion of my testimony.

Improving Analysis

Cross-Agency Integration

Two of the main goals of intelligence reform are to build a sense of community among foreign, military, and domestic intelligence agencies and, through that kind of collaboration, improve the quality of analysis. For greater collaboration to occur, however, analysts must be able to identify and contact peers and counterparts working on related topics.

Prior to the creation of the ODNI, analysts had no easy way to obtain contact information on analysts from other agencies. Today, they have the Analysts Yellow Pages. Launched in February 2006, the Analysts Yellow Pages is a classified, web-based phonebook and a single stop for obtaining contact information on analysts in all IC agencies. It is accessible on the Joint World-wide Intelligence Communications System and allows users to search for analysts across the Intelligence Community by name, by intelligence topic, country, or non-state actor, or by agency. Search results provide contact information including name, agency, phone number, and email address. Our ODNI Chief Information Officer (CIO) is developing a common method to identify, in perpetuity, all the individuals across the IC.

The Information Sharing Environment

Created by IRTPA, the Program Manager for the Information Sharing Environment (PM-ISE), operating in coordination with the interagency under guidelines issued by the President and statutory authority—a well as with strong support from this Committee—has led the charge with our state, local, tribal, private sector, and foreign partners to transform government-wide terrorism-related information sharing policies, processes, procedures, and most important ,workplace cultures, to normalize the sharing of terrorism-related information as part of how we do business.

Section 1016 of the IRTPA and as amended by the 9/11 Commission Act of 2007, established the Office of the Program Manager and provided it with government-wide authority to plan, oversee and manage the ISE. The ISE is a trusted partnership among all levels of government that facilitates the sharing of information relating to terrorism. Creating the ISE is not about building a massive new information system; it is policies, processes/protocols and technology that enable the sharing of this information among Federal, State, local, tribal, private sector entities and our foreign partners.

To guide efforts to establish the ISE and implement the requirements of Section 1016 of IRTPA, on December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies on the *Guidelines and Requirements in Support of the Information Sharing Environment*. In this Memorandum the President prioritized efforts that he believes are most critical to the development of the ISE and assigned to relevant Cabinet officials the responsibility for resolving some of the more complicated issues associated with information sharing.

The PM-ISE in consultation with the Information Sharing Council, State, local, and tribal governments, and private sector partners have made significant progress against the President's priorities in the following areas:

- Development of proposed Common Terrorism Information Sharing Standards (CTISS). The CTISS program develops and issues functional standards that document the rules, conditions, guidelines, and characteristics of business processes, production methods, and products supporting terrorism-related information sharing. (Presidential Guideline 1)

- Establishment of a Federally-sponsored interagency capability in the NCTC to enable the production and dissemination of Federally-coordinated terrorism-related information to state, local, and tribal authorities and the private sector. (Presidential Guideline 2)
- Establishment of a national, integrated network of State and major urban area fusion centers that optimizes our capacity to better support the information needs of State and local authorities, as well as efforts to gather, analyze, and share locally generated information in a manner that protects the information privacy and legal rights of Americans. (Presidential Guideline 2)
- Development of the *Presidential Guideline 3 Report: Standardize Procedures for Sensitive but Unclassified (SBU) Information.* The Report will recommend to the President a new Controlled Unclassified Information (CUI) Framework for rationalizing, standardizing, and simplifying procedures for SBU information in the ISE. (Presidential Guideline 3)
- A repository of information on over 400 unclassified and SBU international information sharing agreements with foreign governments. (Presidential Guideline 4)
- PM-ISE publication of ISE Privacy Guidelines, including development of an implementation guide for Federal agencies. (Presidential Guideline 5)

Although the effort to implement the ISE is well underway, it is essential that implementation activities take place within a broader strategic context of enhancing our Nation’s ability to combat terrorism. The ultimate goal is not simply information sharing for the sake of sharing information. The objective is to improve our national capacity to protect the nation from future attack.

Information Sharing Initiatives within the IC

Initiatives in support of information sharing specifically within the IC include the efforts of the CIO and the ODNI Analysis directorate, to profoundly change how IC components collaborate with each other. We have integrated Internet technologies into the Intelligence Community’s secure and unclassified Intranets, giving individuals the ability to collaborate as groups, peer-to-peer, and in self-identified teams. We are also developing virtual communities of analysts who can securely exchange ideas and expertise across organizational boundaries. Through our pilot Library of National Intelligence initiative, we are providing analysts across the Community a searchable database of disseminated Intelligence products. In a later phase, even if a particular user does not have the clearances to review a desired document, he or she will (in most cases) be advised of the product's existence and offered the opportunity to request access to it.

And analysts are also increasingly using interactive, classified blogs and wikis, much as the tech-savvy, collaboration-minded user would outside the Community. Intellipedia, the IC's version of Wikipedia, and "A-Space" a common workspace environment likened in the press to the commercial website "MySpace," are perhaps the best-known examples. Such tools enable experts from different disciplines to pool their knowledge, form virtual teams, and quickly make complete intelligence assessments.

Efforts to improve collaboration do not stop at the water's edge—literally. Under CIO auspices, we have created the capability for US persons to communicate via email with their Allied counterparts overseas. The solution does not require special networks or equipment but has dramatically changed our capability to share information in a timely manner. The Allied Collaborative Shared Services program and email projects have improved how the US Intelligence Community shares intelligence with our partners.

The underlying principle here is a simple one: no one has a monopoly on truth.

Much the same principle animates our engagement with outside professionals who can challenge our analytic assumptions, provide deep knowledge, insights, and new ways of thinking. Through the Analytic Outreach Initiative, ODNI is expanding networking opportunities for IC analysts and encouraging them to tap expertise on key issues wherever it resides through conferences, seminars, workshops, and exchanges. These outside experts—whether academics, business people, journalists, technical experts, or retired intelligence officers—contribute to proof and validation exercises and to lessons learned processes. They also provide a critical surge capability, especially in areas where IC resources are slim.

We have also taken steps to safeguard the impartiality of our analytic products. As mandated by the IRTPA, the ODNI established an Assistant Deputy for Analytic Integrity and Standards, who serves as the focal point for analysts who wish to raise concerns regarding politicization, bias, or the lack of objectivity, appropriate alternative analysis, or dissenting views in intelligence products. The Office of Analytic Integrity and Standards challenges the IC to evaluate its work and enforce standard that will produce the best possible analytic product for our customers. The AIS is also promoting the use of diverse analytic methodologies. For example, AIS has developed an Introductory Analysis course for new IC analysts, who will receive instruction in critical skills, establish contacts in other agencies, and gain better appreciation of the diversity within the IC.

Many of these improvements would be of little use if they did not reach our customers, including the policymakers of this Committee. Specifically, you may have noticed the qualitative improvements to our National Intelligence Estimates, the IC's most authoritative written judgment on a particular subject. Specifically, NIE Key Judgments no longer contain a list of conclusions but are written to explore more thoroughly the implications of our critical underlying conclusions. Appendices and annexes now provide full transparency of their analytic judgments through the careful identification of sources and intelligence gaps, and by "showing our homework"—essentially, describing the analytic train of reasoning we use to arrive at our conclusions. The main text now highlights the full range of analytic judgments and their implications, bringing dissenting opinions to the fore so policymakers have the benefit of the full picture. We applied many of these lessons learned to the NIE on Homeland Security Threats that I discussed earlier.

Developing a Collaborative Community with a Responsibility to Provide

In the years since 9/11, multiple studies have attributed our inability to prevent the terrorist attacks to the inability or unwillingness of government organizations to share critical information and intelligence fully and effectively. Our success in preventing future attacks depends upon our ability to gather, analyze, and share information and intelligence regarding those who would do us more harm. The intelligence and information sharing structures that enabled the winning of the Cold War need greater flexibility and resilience to confront today's threats from transnational terrorists. Most important, the long-standing policy of only allowing officials access to intelligence on a "need to know" basis should be abandoned for a mindset guided by a "responsibility to provide" intelligence to policymakers, warfighters, and analysts, while still ensuring the protection of sources and methods.

In short, those responsible for combating terrorism must have access to timely and accurate information regarding our adversaries. We must:

- Identify rapidly both immediate and long-term threats;
- Identify persons involved in terrorism-related activities; and

- Implement information-driven and risk-based detection, prevention, deterrence, attribution, response, protection, and emergency management efforts.

Accomplishments Thus Far

In the aftermath of 9/11, our Nation began the historic transformation aimed at preventing future attacks and improving our ability to protect and defend our people and institutions at home and abroad. As a result, we are now better informed of terrorist intentions and plans and better prepared to detect, prevent, and respond to their actions. Improved intelligence collection and analysis has helped paint a more complete picture of the threat, and more robust information sharing has provided us a greater capacity for coordinated and integrated action. Several information sharing successes since 9/11 include the following:

- The enactment of the "USA PATRIOT Act" helped remove barriers that once restricted the effective sharing of information and coordination between the law enforcement and intelligence communities.
- The establishment of the Department of Homeland Security (DHS) and DHS's Office of Intelligence and Analysis has enhanced the sharing of information between federal, state, and local government agencies, and the private sector which in turn has enhanced our ability to detect, identify, understand, and assess terrorist threats both to and vulnerabilities of the homeland to better protect our Nation's critical infrastructure, integrate our emergency response networks, and link state and federal governments. The Chief Intelligence Officer of DHS is now responsible for integrating the intelligence activities of that Department, providing overall guidance on homeland security-specific issues.
- The Terrorist Screening Center was created to consolidate terrorist watch lists and provide around the clock operational support for federal and other government law enforcement personnel across the country.
- The growth and maturation of the 101 Joint Terrorism Task Forces (JTTF) in major jurisdictions throughout the United States, with support from Field Intelligence Groups (FIGs), has substantially contributed to improved terrorism-related information sharing and operational capabilities at the state and municipal levels.

Through these and other efforts, the United States and its coalition partners have made significant strides against al-Qa'ida, its affiliates, and others who threaten us. Collaboration and information sharing have helped limit the ability of al-Qa'ida and like-minded terrorist groups to operate. We have uncovered and eliminated numerous threats to our citizens and to our friends and allies. We have disrupted terrorist plots, arrested operatives, captured or killed senior leaders, and strengthened the capacity of the Nation to confront and defeat our adversaries.

Building a Dynamic Intelligence Enterprise

Joint Duty

Building a collaborative intelligence enterprise goes beyond merely sharing information. It also means fostering a new, Intelligence Community-wide culture without destroying the unique perspectives and capabilities of each agency. In this effort, the IC has a useful model in the Defense Department, which was revolutionized by the Goldwater-Nichols Act of 1986. That Act unified the military establishment and laid the foundations for a “joint” military by establishing incentives for interservice collaboration (such as requiring a joint duty assignment to achieve flag rank) and promoting joint training and development).

Recently, we took a dramatic step toward realizing a similar bedrock shift within the Intelligence Community. Through the authorities granted to the DNI by the IRTPA, I signed a directive mandating civilian joint duty for intelligence officers across the IC. This was a key accomplishment of our 100 Day Plan. Now, if an up-and-coming officer aspires to the senior-ranks of the Community, he or she will have to serve a tour of duty at a different agency during his or her career. The experience provides the officer with a broader perspective and brings the Community a long ways toward the collaborative and unified ideal.

Recruitment Initiatives

Since the establishment of the ODNI, we have been working vigorously to recruit intelligence officers with the backgrounds and skills that will strengthen our security.

The Intelligence Community’s 100 Day Plan for Integration and Collaboration highlighted the need to recruit and retain first- and second-generation Americans with diverse background, critical language skills, and a nuanced understanding of foreign cultures to strengthen the nation’s security. In accordance with initiatives specified in this Plan, the ODNI hosted an inaugural IC Heritage Summit and the first IC Leadership Colloquium in June 2007, beginning a dialogue with national and regional Heritage Community organizations and internal IC affinity groups and special emphasis program leaders. The results from these two events, and the feedback from the external and internal groups, were the foundation for developing the first IC Heritage Community Recruitment, Hiring, and Retention Strategy for first- and second-generation Americans. These groups, as well as our legacy communities, provide a rich pool of diverse talent that has not been consistently tapped into as a source to enable the IC to more accurately reflect the "face" of the American people.

In addition, we have established a formal Intelligence Community Recruiting Subcommittee, consisting of IC Agency Recruitment organizations, that meets regularly to discuss common issues, share best-practices and recruiting successes, plan annual IC collaborative recruiting events, network with leading external recruiting companies and consultants, and recommend solutions to individual IC Agency challenges.

We also developed a centrally funded IC corporate recruiting strategy to recruit collaboratively at national- or high-priority IC target events. Since 2005, the number of events at which we have recruited has more than doubled from 10 to about 25. We pursue a wide-range of applicants by recruiting at a broad array of national career fairs and conferences, including those hosted by: the Society of Hispanic Professional Engineers (SHPE), the National Society of Black Engineers, the American Indian Science and Engineering Society, the Thurgood Marshall Leadership Institute, Women for Hire, and Asian Diversity Career Expos. The IC is also a major sponsor of SHPE and events for the Careers for the Disabled.

Since the enactment of the IRTPA, the IC has established an IC-wide resume database that allows the sharing of resumes from collaborative events and IC Agency referrals and allows recruiters to search for highly-qualified applicants, especially those with desirable backgrounds or language fluencies.

We also established an annual campaign to recruit students from universities deemed Centers for Academic Excellence (CAE). The IC CAE program was established in 2004 to increase the diversity of the IC's applicant pool for entry-level professional positions. The program provides technical and financial support to a diverse cohort of ten specially-selected American colleges and universities so they can develop and deliver degree programs that prepare their graduates for IC jobs in the sciences, information systems and technology, regional studies, and foreign languages.

These initiatives will require follow-on implementation to recruit and hire personnel with the backgrounds and skills considered essential to improve the diversity and ability of the IC workforce, but with continued emphasis and support from the Administration and the Congress, I believe we are well positioned to succeed.

Focused Emphasis on Diversity

I would like to make special mention of the strong support we have received from the Congress in our efforts to diversify our workforce. Representative Silvestre Reyes, Chairman of the House Permanent Select Committee on Intelligence (HPSCI), has, in particular, worked closely with us to promote the recruitment of traditionally underrepresented groups. Chairman Reyes and I both addressed the first IC-wide Affinity Group and Special Emphasis Program Leadership Colloquium in June 2007, and the Chairman hosted a panel on diversity and the Intelligence Community last month in El Paso, Texas with Jose A. Rodriguez, the outgoing director of the CIA's National Clandestine Service.

We have also completed the first IC EEO and Diversity Strategy (Five-Year Plan for 2007-2012) as a priority initiative in our 100 Day Plan, responding to the HPSCI mark draft language and addressing a fundamental need to ensure that the IC workplace continues to be characterized by fairness and equality. Without such assurance, we cannot expect to attract and retain a workforce that looks like America and can operate in a global threat environment. Furthermore, our IC hiring and promotion practices must at least equal, and preferably surpass, other government agencies in transparency and equity if the American people are to willingly extend to us the latitude absolutely necessary to protect our nation.

Security Reform

The recruitment and hiring of first- and second-generation Americans brings into sharp relief a weakness that has plagued the Intelligence Community for decades: the onerous security clearance process required to work in the IC. The IRTPA mandated the reformation of security clearance procedures, and it remains one of our top priorities.

As someone who has worked in the private sector and been exposed to the other side of the security clearance process, I can speak from experience of the frustration that often accompanies lengthy and seemingly unnecessary delays in getting individuals cleared for duty.

Accordingly, we identified security clearance reform as a top priority for the 100 Day Plan and established a Tiger Team at the ODNI Special Security Center to lead this crucial reform. We are undertaking this security reform initiative jointly with the Department of Defense. We have designed a transformed clearance process and developed a plan to assess the validity of this process.

The comprehensive reform of the security clearance process remains our ultimate goal in order to deliver high-assurance security clearances, fairly, efficiently, and at the lowest possible cost. The new process will be based upon end-to-end automation, new sources of data, analytical research, and best practices. Some of these pieces already exist in the Community but they need to be integrated into a single process.

Foreign Language Initiatives

To build a strong foundation for the future of the Intelligence Community, we must also increase foreign language capacity among our workforce and support the study of languages among America's youth. To that end, ODNI is sponsoring a major Intelligence Community study of how to optimize foreign language staffing, taking into account language and proficiency requirements, retention, training, and cost, and comparing the roles played by civilian, military, and contractor personnel in performing foreign language tasks. The study is being conducted by the RAND Corporation and initial results are expected in 2008.

The ODNI also purchased a Community license for on-line language training software in 150 languages. All IC personnel will be able to utilize this resource. We are also supporting several research projects to improve the effectiveness of foreign language training, including evaluations of both commercially-developed and government-sponsored on-line language training programs.

Furthermore, ODNI has initiated a new collaborative program, called the Language Education and Resources Network to share best teaching practices and learning materials in critical languages developed in language schools throughout the U.S. government. Major workshops have been held in Chinese and Arabic, with additional workshops planned in Persian, Hindi, Urdu, and Korean within the next year.

We have also sponsored conferences and facilitated information sharing to enhance key capabilities in human language technology, such as machine translation and content extraction. ODNI is developing a Human Language Technology Roadmap, to guide and prioritize investment across the IC.

To fill critical gaps, ODNI is spearheading an initiative to create temporary hiring billets, to speed up the on-boarding process for applicants with outstanding foreign language skills, including heritage community applicants. Temporary billets could be used to hire personnel who are awaiting clearance and allow them to work in unclassified settings, such as open source research, or to permit placement of personnel who have been cleared, but for whom no permanent billet is immediately available.

Finally, ODNI—in partnership with the National Security Agency—leads STARTALK, a new program in summer language education. A part of a Presidential initiative to improve critical language skills, STARTALK will provide funding for programs in over 20 states and Washington D.C. to educate both students and language teachers. The classes focus on Arabic or Chinese and range from week-long tutorials to nine-week immersions. Through this program, hundreds of young people will receive education that will enrich their lives, enhance their futures, and strengthen our nation's global competitiveness—yielding substantial returns for an initial investment of only five million dollars.

Looking to the Future

The passage of the IRTPA and the creation of the DNI were important steps toward building an integrated and collaborative Intelligence Community that is well positioned to defend the nation—but they must be part of a larger reform effort.

To support the IC vision of integration and collaboration we initiated a deliberate planning process based on the principles of transparency, accountability, deadlines, and deliverables. The first phase of these efforts—the recently completed 100 Day Plan—was designed to jump-start the process and build momentum. The next phase—the 500 Day Plan—is intended to sustain and accelerate that energy with an expanded set of initiatives and a greater level of participation. This latter plan was developed through a Community-wide effort beginning last May through the use of working groups, blogs, and wikis to solicit input from the Community. During our coordination process, we identified several core priorities and over 30 supporting initiatives. The core initiatives represent major long term impact projects that will be monitored and reported on a biweekly basis to my office and reviewed by the EXCOM monthly; they represent “major muscle movements”—something required for this transformational effort.

The 500 Day Plan will be executed through cross-organizational and Community-wide engagement and collaboration. Working groups for each initiative will include key stakeholders from throughout the Community. It is through implementation of these initiatives that the IC will continue to increase its efficiency and effectiveness and further meet the national security challenges of the 21st century.

Protect America Act of 2007

Finally, I would like to make note of an issue on which I hope the Congress takes action in the coming months. The recent enactment of the Protect America Act of 2007 provided a necessary update to the Foreign Intelligence Surveillance Act (FISA). This critical legislation has already assisted the IC in closing a critical gap in the IC’s ability to provide warning of threats to the country. This Act sunsets in less than six months, and I believe that making its changes permanent will be an important step toward ensuring the protection of our Nation. Importantly, the Act provides for meaningful oversight of activities. The Department of Justice’s National Security Division, IC general counsel offices, and the ODNI Civil Liberties and Privacy Office, in addition to existing oversight mechanisms within the IC, will all be involved in overseeing implementation of the Act's authorities.

I am committed to keeping the Congress fully and currently informed of how this Act has improved the ability of the Intelligence Community to protect the country and look forward to working with the Congress to obtain lasting FISA modernization.

Conclusion

In closing, we have come a long way over the past six years developing a more integrated, more collaborative intelligence enterprise, and I believe the result has been a stronger Community better positioned to know the world and anticipate surprise. While we have seen success in our efforts to **structure** the Intelligence Community to meet 21st century challenges; **improve** analysis; develop a **collaborative** Community that provides the right information to the right people at the right time; and **build** a dynamic intelligence enterprise that promotes diversity to gain and sustain a competitive advantage against our adversaries, our work is far from done.

With your support, I look forward to building a legacy of reform that will outlast our own time and provide for the protection of the Republic in the decades to come.

Mr. Chairman, this concludes my remarks. I welcome any questions you may have. Thank you.