

Statement for the Record of

CHARLES E. ALLEN

**Under Secretary for Intelligence and Analysis
Chief Intelligence Officer
Department of Homeland Security**

“Information Sharing at the Federal, State, and Local Levels.”

U.S. Senate

Committee on Homeland Security and Governmental Affairs

July 23, 2008

Thank you, Chairman Lieberman, Ranking Member Collins, and Members of the Committee for the invitation to appear today. I know that information sharing has long been of special interest to this Congress and that your Committee played an integral role in directing the President to create an Information Sharing Environment for the sharing of terrorism information as part of the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act). So, I am pleased to have the opportunity to tell you about the real progress that the Department of Homeland Security, in cooperation with its Federal, State, local, tribal, territorial, and private sector partners, has made to ensure that the words “information sharing” are not a phrase repeated for political effect but rather reflect the inextricable relationship of information sharing to the primary DHS mission. I will explain how the Department is weaving information sharing into the fabric of its operations. Information sharing is an enabling function and core responsibility of every Departmental element, and as a result, will continue to improve regardless of transitions in leadership and organization.

The Department has heeded the calls from the President, as detailed in his *National Strategy for Information Sharing*, and the Congress to increase information sharing across the homeland security enterprise and create a culture based on the “responsibility to provide” information. But we recognize ensuring information gets to the right people does not happen automatically and cannot be left to chance. It requires dedicated efforts and constant attention as well as creating systems, processes, and environments that make sharing easier and more productive.

We have a statutorily mandated role in information sharing as prescribed by the Homeland Security Act of 2002. Creating the cultural and organizational infrastructure necessary to enhance the information sharing capabilities of the Department is a critical DHS mission to which we have devoted substantial resources. The efforts for improving information sharing throughout the Department are manifested in dozens of policies, mandates, and strategies issued since the Department was established and we are seeing results from these foundational efforts. One seminal policy regarding information sharing is the *DHS Policy for Internal Information Exchange and Sharing* that was signed by Secretary Chertoff on February 1, 2007. Referred to in the Department as the “One DHS” memorandum, its purpose is to promote a cohesive, collaborative, and united Department-wide information sharing environment to reflect and complement the Department’s similarly unified mission. The issuance of this memo provided essential direction to all of the Department’s components and organizations to share information as part of a single enterprise. The Secretary expanded on his One DHS policy in May 2008 when he issued the *DHS Information Sharing Strategy*, which provides strategic direction and guidance for all DHS information sharing efforts, both internally and with external stakeholders, including Federal, State, local, tribal, private sector, and international partners.

While Ambassador McNamara has provided you with the state of the Information Sharing Environment writ large and the respective policies that have been put in place since the passage of the Intelligence Reform Act, I want to focus on how these concepts are being translated into action in this Department. I want to illuminate how the Department is building an information sharing governance structure to ensure the entire DHS enterprise can speak with one voice, and bring all of its information and knowledge to bear on preventing, protecting against, and

responding effectively to threats against our homeland. I also want to describe the significant progress the Department has made in working with our Federal partners – most notably the DOJ/FBI, the DNI, and NCTC – to ensure that the Federal government is working in concert on these issues to maximize the benefit of our actions. Finally, I want to describe the myriad of ways DHS and our Federal partners work with our non-Federal partners to ensure that information is gathered and shared among all of us working to protect our country and all who live here.

DHS recognizes that a strong foundation is essential to long-term, sustainable improvements in information sharing. The governance structures we have built within DHS with my leadership as the Chief Intelligence Officer and the DHS Executive Agent for Information Sharing provide the essential foundation for the robust information sharing effort that our unified mission demands.

In April 2007, the Secretary established an Information Sharing Governance Board (ISGB) to serve as the executive level steering committee and decision-making body for all information sharing and collaboration activities within the Department. I currently serve as chair for the ISGB. Other members currently include the principal leaders of the Offices of Policy and International Relations, Intelligence and Analysis (I&A), Operations Coordination, Infrastructure Protection, the Chief Information Officer, the General Counsel, and the designated Lead for the Law Enforcement Shared Mission Community, or LE-SMC (a rotating position presently encumbered by the Assistant Secretary for Immigration and Customs Enforcement). In addition, our Chief Privacy Officer and several other senior Departmental officials serve as *ex officio*

members. The ISGB is the organization empowered to exercise the Secretary's ultimate decision-making responsibility on information-sharing matters.

Second, we have formed the DHS Information Sharing Coordinating Council (ISCC), an advisory, action-oriented body, fully representative of the Department's many organizational elements, that provides working-level deliberation and support to the ISGB. The ISCC is composed of Action Officers independently assigned by each of the Department's components and offices to represent their respective interests and perspectives. Among its many other responsibilities, this is the body that initially tackles the issues and tasks that are sent to the Department from the government-wide Information Sharing Environment.

Third, we are establishing Shared Mission Communities (SMCs) within DHS. The SMCs are cross-cutting information sharing efforts that bring together all of the relevant organizations within DHS that share common missions and objectives. They address the need to build integrated cultures, processes, and policies that facilitate information sharing across internal organizational boundaries.

The Law Enforcement Shared Mission Community (also known as the LE SMC) was the first shared mission community to be established and unites the full breadth of DHS law enforcement entities to enhance information sharing between components, other Federal agencies, and State, local and tribal law enforcement entities. This initiative has enabled the Department to create the Law Enforcement Information Sharing Service (LEIS Service) pilot, which unites DHS components and other Federal agencies to provide a single point of entry for Federal information

sharing. Over time, this initiative will provide significant cost and resource savings (thereby reducing operational costs) including to the Department and our State and local partners and deliver benefits while standardizing methods and policies. These benefits include providing improved law enforcement information sharing, which will result in increased officer safety and enhanced law enforcement operation effectiveness to deliver on the Department's mission to protect and prevent threats against the general public and the Nation as a whole.

The LEIS Service allows for the effective and appropriate sharing of DHS law enforcement data with State and local authorities through the deployment of information sharing technologies and operating policies. This technology complies with the President's *National Strategy for Information Sharing* and is aligned to the Information Sharing Environment (ISE) architecture framework. Additionally, the LEIS Service has collaborated with the Department of Justice (DOJ) to leverage their existing OneDOJ network in locations where it is cost effective and begin to build the backbone of a unified Federal infrastructure, thereby avoiding duplicative costs incurred by building independent infrastructures. Additionally the LE SMC has collaborated with the Departments of Defense and State to determine if additional economies of scale exist. This initiative will enable the eventual establishment of one standard for information sharing across federal law enforcement entities.

The LEIS Service has been developed using the ICE Pattern Analysis and Information Collection (ICEPIC) system to share excerpts from subject records and closed cases. Additionally, memorandums of agreement have been established to ensure consistent governance with State, local and tribal partners. The service has been launched this year in San Diego and Los Angeles

with favorable initial results. The LEIS Service is also scheduled for deployment in Arizona and Texas by the end of this year. A long term deployment schedule, including the National Capitol Region and Chicago, is under development.

While the Department's unified governance structure, consisting of the ISGB and ISCC, is the essential foundation for fulfilling the Department's information sharing mission requirements, achieving the mission requires people and tools. We have devoted significant resources to providing both of these. There is no place where this is more evident than our efforts to ensure a two-way flow of information between our State, local, tribal, territorial, and private sector partners and the Federal government. As the Implementing the Recommendations of the 9/11 Commission Act (9/11 Commission Act) and the President's *National Strategy for Information Sharing* make clear, fusion centers are an essential part of this information flow and framework. Working closely with the Department of Justice, DHS has critical responsibilities for leading the Federal effort to work with States and major urban areas to establish fusion centers across the country and design policies and programs to integrate them into a national network. Fusion centers form a critical bridge for sharing information vertically between the Federal government and our partners, as well as horizontally across the States. DHS has taken the lead to integrate the fusion centers into the Information Sharing Environment.

I am the Department's Executive Agent for support to the fusion centers. Within my Office of I&A, my team established the Department's State and Local Fusion Center Program Management Office (SLPMO) to build essential relationships with the fusion centers. By the time the 9/11 Commission Act passed late last year and called for the establishment of a fusion

center program office within the Department, the SLP MO was already operational and had been since June 2006, when the Secretary signed The Department of Homeland Security Support Implementation Plan For State and Local Fusion Centers.

As a Department we support fusion centers by deploying, through the SLP MO, DHS intelligence officers to the centers, providing grant funding for their development and operation, connecting networks and systems, and strengthening the relevant communities of interest. To date we have 25 officers deployed and serving in fusion centers and we plan to have 10 more deployed by the end of this year. These men and women serve at the front line for information sharing. By using their varied experiences and skills as intelligence professionals, they are providing State, local, tribal, territorial, and even other Federal partners with the information they need to keep America safe. These same skills permit them to cull the best of what fusion centers are collecting and analyzing and ensure that it gets to the appropriate people in other States and in the Federal government – building the National Fusion Center Network.

To ensure that the National Fusion Center Network is staffed by analysts across the country who make the best use of their access to National-level intelligence, my Office is providing or coordinating intelligence training at the fusion centers. In a mobile training format we have delivered the one-week long Analysis and Critical Thinking Skills Workshop to over 40 analysts; another 20 are receiving this training this week as we speak. Our plan is to get this training to an additional 140 analysts over the next year. Through the Office of the DNI, we are taking advantage of its Open Source Academy's classes as well. The Academy has provided several sessions of the week-long Introduction to Analytic Tradecraft and the 2-day Tools and

Techniques classes directly to several fusion centers. We are also working to make the Basic Intelligence Threat and Analysis Course (BITAC) and the DNI's Analysis 101 available to as many State, local, and tribal analysts as we possibly can.

In addition to ensuring that the right people are in place to analyze the information that is being provided, DHS is committed to providing fusion centers with the information sharing tools they need to participate in the Information Sharing Environment. To do so, we are providing network connectivity at the classified and unclassified level that enables fusion center personnel, both our own DHS officers as well as State and local analysts, access to Federal systems and data sources.

At the Secret level, we are deploying the Homeland Secure Data Network (HSDN). To date, HSDN has been deployed to 23 fusion centers and we are working to deploy it to 17 more by the end of this year. Our primary constraint in achieving this goal is ensuring that enough fusion centers have upgraded their facilities and infrastructure to the necessary security standards for deployment of classified systems. Among other capabilities, HSDN provides access to NCTC On-line – a classified portal that maintains the most current terrorism-related information at the Secret level. HSDN also provides the fusion centers with a window into the National Intelligence Community that they can use for their own information needs, as appropriate. Ultimately, every State and Local Fusion Center (SLFC) with HSDN access will have its own webpage to which relevant State, local, and tribal products can be posted and made available to other fusion centers and broader communities, including the National Intelligence Community.

On the unclassified level, the Homeland Security Information Network's "Intelligence" portal (HSIN-Intelligence) provides more than 8,000 people with access to finished FOUO intelligence products. To foster collaboration and share best practices and lessons learned within the fusion center network, DHS sponsors the Homeland Security State and Local Intelligence Community of Interest (HS SLIC), a virtual community of intelligence analysts. Its membership has grown significantly in the past year and now has members representing 43 States, the District of Columbia, and seven Federal departments. I have also established a HS SLIC Advisory Board, which includes State and local leaders of the HS SLIC to advise me and the rest of I&A leadership on issues relating to intelligence collaboration with our non-Federal partners. Through the HS SLIC, intelligence analysts across the country collaborate via weekly FOUO threat teleconferences, bi-weekly Secret-level secure video teleconferences, and in a virtual community of interest within a restricted portion of the HSIN-Intelligence platform, to share intelligence information in an appropriately secure and privacy sensitive environment. Members are thus able to post intelligence products so that there is effective vertical information sharing between the States and the Federal Intelligence Community and horizontally between the States. In addition, I have established an HS SLIC conference series which includes both an annual nationwide analytic conference conducted at the Secret level each September, and at least one annual theme-oriented conference per region, also at the Secret level. Finally, we are also planning to introduce on HSDN a secure, virtual collaboration workspace capability similar to that now available to the HS SLIC within HSIN-Intelligence. This connectivity will further enable us and our partners to collaborate more effectively and efficiently at the Secret level. Through all of these varied activities, DHS is making the HS SLIC a significant contributor to the National Strategy for Information Sharing.

In addition to the network connectivity we are providing to fusion centers, the Department has also developed the Constellation / Automated Critical Asset Management System (C/ACAMS), a tool that supports fusion centers and other information sharing partners in support of the Department's mission of protecting critical infrastructure. C/ACAMS provides State, local, and private sector partners with a set of resources to collect and manage information related to critical infrastructures and to inject infrastructure information into fusion center analysis. This information, when combined with terrorism threat streams, provides fusion center analysts and private sector infrastructure owners and operators with a context to understand risk and to target protection resources against those assets or systems with the highest risk profiles. C/ACAMS is currently deployed to fusion centers across the country and is used by over 2,000 State and local infrastructure protection analysts. The data they have collected on over 38,000 unique infrastructure assets is vital to the national effort to enable prevention, protection, response, and recovery activities.

DHS is working to ensure that the information we share is what our partners need. To further this effort we undertook a pilot project with six fusion center partners to examine the day-to-day information needs of the centers. By working with the DHS officers embedded in the fusion center, intelligence personnel at DHS headquarters and, most importantly, our State and local partners, my Office was able to develop a precise set of priority information needs for fusion centers.

The leader of this pilot said in his report that there was a need for clearer paths for information flows and greater participation by the State and local personnel in the development of the information. As a result of these insights, we changed how information flowed within the Department and created a single point of service for supporting our State, local, and tribal partners. By identifying a single access point within the Department and bringing broad departmental support to the fusion centers through the DHS National Operations Center, DHS mitigates the confusion our State, local, and tribal partners faced of how best to interface with a department of our size and complexity. Moreover, we are now seeing joint analytic products serving all levels of government and the private sector being written by fusion centers in conjunction with DHS and FBI. So far, this year, nine finished intelligence products were co-authored by DHS, fusion centers, and other partners. In addition, more than 150 Homeland Intelligence Reports (DHS intelligence products designed to take information collected by DHS and share with the broader national Intelligence Community) have been written this year, using information DHS has obtained from its State, local, and tribal partners. We would not have obtained this information, except through this critical partnership. Collaboration such as this is precisely what the Congress and the president envisioned in directing our Nation's intelligence and law enforcement communities to improve information sharing.

Although my Office leads the Department's fusion center efforts, we are reaching out across the DHS enterprise to bring all of the Department's resources to bear. As one example, the SLPMO has close relationships with FEMA's Technical Assistance Branch and works together to provide a broad range of support to the fusion centers. FEMA and the Department of Justice's Bureau of Justice Assistance have created the Intelligence Liaison Officers Program and the Terrorism

Liaison Program which are designed to ensure that information contained within the fusion centers reaches the street level police officer and firefighter, and just as important, provides them with a clearly defined pathway for providing information back to the center and through it to the Federal level. Grant and technical experts from both Departments jointly administer these programs.

In addition to these specific DHS initiatives, the Department is providing leadership to important multi-agency organizations dedicated to improving information sharing with our non-Federal partners.

An important piece of multi-organizational effort is the National Fusion Center Coordination Group (NFCCG) that was established as a working group under the Information Sharing Council, to assist the implementation of the recommendations approved by the President, and later incorporated into the *National Strategy for Information Sharing*, to establish a national integrated network of fusion centers. The director of my State and Local Fusion Center Program Management Office serves as co-chair of this important group with the Deputy Director of Intelligence at the FBI. The Group brings together key Federal partners from the FBI, DOJ, DHS, DNI, PM-ISE, as well as State and local organizational leaders to build the framework needed for effective information sharing.

The NFCCG has been successful in fostering the development of fusion centers and bringing them into a cohesive partnership at the State and local level as well as with their Federal partners.

One notable achievement of this Group is its coordination and sponsorship of a series of national and regional fusion center conferences. The two national conferences to date are widely considered by fusion center managers and personnel to have been highly productive and successful. Nearly 600 delegates attended in 2007 and we reached capacity this year at almost 900 attendees, with several hundred interested participants turned away. This has become the seminal information sharing conference for State, local, and tribal governments, fusion centers, and their Federal partners.

On the content side of this effort, the Interagency Threat Assessment and Coordination Group (ITACG) was established at the direction of the President and the 9/11 Commission Act to facilitate increased sharing of terrorism-related information between the National Intelligence Community and our State, local, tribal, territorial, and private sector partners. Too often in the past our non-Federal partners were confused by seemingly inconsistent information coming from various parts of the Federal government or complained that they lacked threat warning and assessment information. By pulling together in one place State, local, tribal, territorial, and Federal homeland security, law enforcement, and intelligence officers at the National Counterterrorism Center, there is now a focal point to guide the development and dissemination of Federal terrorism-related intelligence products through DHS and the FBI to our State, local, tribal territorial, and private sector partners.

Under law, the ITACG consists of two elements: the ITACG Detail and the Advisory Council. The Detail is the group of individuals who sit at the NCTC and conduct the day to day work of the ITACG. The Council is tasked with setting policy and developing processes for the

integration, analysis, and dissemination of Federally coordinated information, as well as for providing oversight of the ITACG Detail and its work.

The Detail achieved Initial Operating Capability just six months ago on January 30, 2008. While fully integrated into the work and leadership at NCTC, the Detail is led by one of my senior intelligence officers who serves as the ITACG Director. The Deputy Director is a senior analyst from the FBI. The FBI and my Office have each provided an additional senior analyst to help with the operation of the Detail. Currently there are four law enforcement officers from State and local police departments, a tribal representative who works at NCTC, and two NCTC contractors with extensive experience in the intelligence community and State and local law enforcement. These non-Federal participants are assigned to assist the Detail and provide critical insight into the needs and perspectives of our State, local tribal and private sector partners. We are working hard to expand the number of non-Federal participants to ten in order to include a broad range of expertise, including fire and health departments, homeland security advisers, and other organizations as needed. Even as we seek to expand the membership of the IATCG, our primary focus remains on strengthening the ITACG by ensuring effective State and local law enforcement representation.

The members of the Detail have essential systems connectivity in NCTC, participate in key briefings, and are engaged in the NCTC production processes and activities so they have the broad perspective of the Intelligence Community. They can then act as an advocate for our State, local tribal and private sector partners by informing and shaping National Intelligence Community products to better meet the specific needs of the State, local tribal and private sector

entities. They support the production of three types of reports: 1. alerts, warnings, notifications, and updates of time-sensitive information related to terrorism threats to locations within the United States; 2. situational awareness reports regarding significant events or activities occurring at the international, National, State, local, or tribal levels; and 3. strategic and foundational assessments of terrorist threats to the United States. In the event of conflicting reporting or, as the need arises, the ITACG facilitates Federal coordination to ensure that reporting on threat information is clear and actionable to the greatest extent possible.

The ITACG Detail has reviewed tens of thousands of finished intelligence products. As part of the review, the ITACG identifies products that meet State, local, and tribal needs, and ensures that they were disseminated appropriately to State, local, and tribal officials. The group has also reviewed thousands of separate reports on worldwide threats to U.S. interests, identifying those that were possible threats to the Homeland. For a small number of these, the ITACG Detail revealed that the reports were of questionable credibility, some of which required better characterization of the threat or source. As a direct result of the ITACG's efforts, DHS and FBI refined their characterization of the threat and released joint reports on two cases that required further threat detail.

We have also established the ITACG Advisory Council that I chair on behalf of the Secretary. The Council, at least 50 percent of whose members must represent State, local, and tribal organizations, has become a robust organization. Although the 9/11 Commission Act requires that it meet a minimum of four times a year, its work is too important and too pressing to meet so infrequently. Instead, we meet in person every other month. Four such meetings have been held

to date. In the months when we do not meet in person, we hold a teleconference. This way critical issues and tasks do not linger before being tackled and resolved. These meetings address a number of priority challenges that we expect this new organization to face – especially recruitment of outstanding State, local, and tribal personnel to serve on the Detail, establishing an attractive Fellowship Program for the selected detailees, and developing formal mechanisms to ensure that information is getting to the right customers and creating a feedback process for State, local, tribal and private sector customers. Although progress on these issues has been slower than I wanted, we are starting to make major breakthroughs that will move the ITACG forward and ensure that it excels at its mission. I am proud of the team we have assembled – both for the Detail and the Advisory Council – and appreciate their continuing contributions to this critical work.

DHS also is working with its Federal partners on a number of less visible but still very important efforts to improve information sharing. I want to highlight two notable examples of initiatives that are enhancing our capabilities: National Information Exchange Model (NIEM) and suspicious activity reporting (SAR).

In the last twelve months DHS has dramatically increased its adoption of the National Information Exchange Model (NIEM). NIEM is a data standards management initiative co-sponsored by the Departments of Homeland Security and Justice with extensive participation by State and local stakeholders. The implementation of the NIEM standard in an information technology (IT) system enables data to be translated into a common language and shared more easily with other IT systems. This effort is essential because without data standards, system-to-

system data exchanges are often difficult, both within agencies and with external partners. Data standards like NIEM not only enhance our ability to connect the dots that exist in numerous IT systems, they also enhance our ability to categorize data and ensure appropriate user access and usage in accord with privacy and civil liberties rules.

Across the Department, components such as CBP, FEMA, ICE, NPPD, S&T, TSA, USCIS and US-VISIT are realizing these opportunities through NIEM adoption within major IT investment programs. These opportunities, such as those being built at ICE in support of law enforcement information sharing, will improve the way information is shared with State, local and tribal partners. Additional opportunities will include improving screening against the terrorist watchlisting, defining exchanges in support of radiological nuclear detection systems, and the creation of person-centric query capabilities that will enable agencies, such as USCIS, to gather information from DHS and Department of State systems to build a comprehensive picture of an individual to support immigration benefit determination process.

NIEM adoption is also happening at the State and local level. As part of the Homeland Security Grant Program, DHS requires all grantees to use the latest NIEM specifications and guidelines regarding the use of Extensible Markup Language (XML) for all HSGP awards. DOJ has the same requirement for several of its grant programs. Far from resisting this imperative, our State and local partners are embracing the adoption of NIEM because it enables information sharing with Federal government systems and across State and local jurisdictions.

In early July, the HSIN-Intelligence platform began establishing, in coordination with the Department of Justice and the Program Manager for the Information Sharing Environment, federated access capabilities across a number of other information sharing platforms such as Law Enforcement Online (LEO) and the Regional Information Sharing System Network (RISSNet). For the first time, DHS has allowed appropriate Department of Justice users of these other platforms direct access to DHS finished intelligence products residing on HSIN-Intelligence without requiring separate password or login requirements. By making access to multiple systems easier, we hope to reduce the gaps in knowledge that might occur from accessing only one system.

In addition, DHS and its Federal partners have made significant progress in their efforts to coordinate an effective, unified strategy for the handling of suspicious activity reporting (SARs). Using SARs has been identified as a capability to begin to see seemingly disparate activities that, when overlapped, show a pattern and possible threats. By designing a system that incorporates procedures and actions that begin at the State, local, and tribal levels, and are supported at the Federal level, DHS' ability to review, analyze, and further disseminate important information that is collected by non-Federal partners is significantly enhanced.

Across the country, DHS has worked closely with local jurisdictions, including Los Angeles, Miami, Boston and Chicago, to understand their approach to SARs and how to best promote cross-integration. By identifying "best practices" at the State, local, and tribal levels, the Federal partners are able to build a collaborative SAR approach.

All of the Federal activities in SARs continue to carefully maintain the balance between the protection of its citizens and the protection of its citizen's privacy and civil liberties. There are standing working groups and committees involving the General Counsel, Privacy, and Civil Rights / Civil Liberties Offices, of the Federal Departments involved in suspicious activity reporting.

We must remember, however, that increased information sharing comes with responsibilities.

We are ever mindful that all of these efforts discussed today must be conducted with civil liberties and privacy rights at the table. To that end, our Privacy and Civil Rights Offices have delivered training to all of our deployed officers and are working with Bureau of Justice Assistance and PM-ISE to develop training for State, local, and tribal representatives in the fusion centers. We are also developing Privacy Impact Assessments for these efforts.

While these particular accomplishments of these inter-agency organizations such as the NFCCG and the ITACG and these other examples of multi-agency collaboration are important in their own right, they are particularly notable because of the close relationships among DHS, FBI, DOJ, the DNI, the PM-ISE, and the many State and local leaders that make them possible. It is these relationships in conjunction with the framework that is being created that makes information sharing a routine occurrence rather than a special event.

Conclusion

I have touched on a broad range of information sharing activities involving the Department and its valued partners because I wanted to give the Committee a sense of the extraordinary efforts DHS is making to foster information sharing at all levels of government. Information sharing is not, and cannot, be an afterthought or a sideline activity. It is not merely incidental to, but rather essential to and, indeed, a vital piece of our mission. We remain committed to implementing the information sharing mandates of the Intelligence Reform and Terrorism Act of 2004, the Homeland Security Act of 2002, and the recently passed 9/11 Commission Act, while continuing to protect civil liberties and privacy.

Thank you and I look forward to your questions.