Testimony of

Thad W. Allen
Admiral, U.S. Coast Guard (retired)

U.S. Senate
Committee on Homeland Security and Government Affairs

The Department of Homeland Security at 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats

Wednesday September 11, 2013
342 Dirksen Senate Office Building

Mr. Chairman, Ranking Member Senator Coburn, and members of the committee, I am pleased to have been invited to testify on this important topic and I thank you for the opportunity.

For the record I am testifying in my personal capacity today and am not representing any other entity.

I am also pleased to be here with my distinguished colleagues Secretary Tom Ridge and former Congresswoman Jane Harmon, both of whom have served their country with distinction. I consider them friends and role models.

Mr. Chairman, in the last year we have witness three key anniversary dates in the history of the Department of Homeland Security. The Homeland Security Act was signed into law by President Bush on 25 November 2012. The Department came into existence on 24 January 2003. Finally, the agencies and functions from legacy departments were transferred to the Department on 1 March 2003, completing the statutorily mandated actions to create the Department.

The Past and Present

In prior testimony before this committee I have provided my personal view of the creation of the department and the implications of the compressed timeframe between the signing of the legislation and the first day of full operations, barely more than three months. While this could be considered government at light speed, little time was available for deliberate planning and thoughtful consideration of available alternatives. The situation was complicated by the fact that the law was passed between legislative sessions and in the middle of a fiscal year. Other than Secretary Ridge, early leadership positions were filled by existing senior officials serving in government and did not require confirmation. Funding was provided through the reprogramming of current funds from across government for departmental elements that did not have existing appropriations from their legacy departments.

Operating funds for components that were transferred were identified quickly and shifted to new accounts in the Department to meet the deadline. Because of the wide range of transparency and accuracy of the appropriation structure and funds management systems of the legacy departments some of the new operational components faced a number of immediate challenges. Estimating the cost of salaries for Customs and Border Protection (CBP) or Immigration and Customs Enforcement (ICE) required the combination of different work forces, with different grade structures, different career ladders, and different work rules.

Basic mission support functions of the department such as financial accounting, human resource management, real property management, information resource management, procurement, and logistics were retained largely at the component level in legacy systems that varied widely. Funding for those functions was retained at the component level as well. In those cases where new entities were created (i.e. Departmental level management and operations, the Under Secretary for Science and Technology, the Under Secretary for Intelligence and Analysis, the Domestic Nuclear Detection Office) support systems had to be created rapidly to meet immediate demands of mission execution. Finally, components and departmental offices that did not preexist the legislation were located in available space around the Washington DC area and the Secretary and number of new functions were located at the Nebraska Avenue Complex in Northwest Washington.

At the time of this transition I was serving as the Coast Guard Chief of Staff and was assigned as the Coast Guard executive to overseas the Service's relocation from the Department of Transportation to the new Department. We began planning for eventual relocation as soon as the administration submitted legislation to the Congress. I also assigned personnel to the Transition Planning Office (TPO) that was created in the Office of Management and Budget by Executive Order to prepare for the transition. A considerable challenge during this period was the fact that the TPO was part of the Executive Office of the President and there were legal limitations on how much of their work could be shared externally. As a result much of that effort was redone or duplicated when the Department was created.

My intent is not to dwell on the past but to frame the degree of difficulty facing the leaders attempting to stand up the Department from the outset. Many of these issues persist today, ten years later. Despite several attempts to centralize and consolidate functions such as financial accounting and human resource management, most support functions remain located in departmental components and the funding to support those functions remains in their appropriations. Because of dissimilarities between appropriations structures of components transferred from legacy departments there is a lack of uniformity, comparability, and transparency in budget presentations across the department. As a result it is difficult to clearly differentiate, for example, between personnel costs, operations and maintenance costs, information technology costs, and capital investment. Finally, the five-year Future Years Homeland Security Plan (FYHSP) required by the Homeland Security Act has never been effectively implemented as a long rang planning, programming, and budgeting framework inhibiting effective planning and execution of multi-year acquisitions and investments.

In the Washington Area the Department remains a disjointed collection of facilities and the future of the relocation to the St. Elizabeth's campus remains in serious doubt. One of the great opportunity costs that will occur if this does not happen will be the failure to create a fully functioning National Operations Center for the Department that could serve at the integrating node for departmental wide operations and establish the competency and credibility of the Department to coordinate homeland security related events and responses across government as envisioned by the Homeland Security Act. As with the mission support functions discussed earlier, the Department has struggled to evolve an operational planning and mission execution coordination capability. As a result, the most robust command and control functions and capabilities in the Department reside at the component level with the current NOC serving as a collator of information and reporting conduit for the Secretary.

The combination of these factors, in my view, has severely constrained the ability to the Department of mature as an enterprise. And while there is significant potential for increased efficiencies and effectiveness, the real cause for action remains the creation of unity of effort that enables better mission performance. In this regard there is no higher priority than removing barriers to information sharing within the department and improved operational planning and execution. Effective internal management and effective mission execution require the same commitment to shared services, information systems consolidation, the reduction in proprietary technologies and software, and the employment of emerging cloud technologies.

Looking to the future the discussion should begin with the Department's missions and whether they adequate reflect the needs of the Nation ten years later … and the need to create unity of effort internally and across the homeland security enterprise.

The Quadrennial Homeland Security Review

The Quadrennial Homeland Security Review was envisioned as a vehicle to consider the Department's future. The first review completed in 2010 described the following DHS missions

- Preventing Terrorism and Enhancing Security
- Securing and Managing Our Borders
- Enforcing and Administering our Immigration Laws
- Safeguarding and Security Cyberspace
- Insuring Resiliency to Disasters

An additional area of specific focus was the maturation of the homeland security "enterprise" which extends beyond the department itself to all elements of society that participate in and contribute to the security of the homeland.

The QHSR outcomes were consistent with the fiscal year 2010 budget that was submitted in early 2009 following the change of administrations. That request laid out the following mission priorities for the Department

- Guarding Against Terrorism
- Securing Our Borders
- Smart and Tough Enforcement of Immigration Laws and Improving Immigration Services
- Preparing For, Responding To, and Recovering From Natural Disasters
- Unifying and Maturing DHS

The FY 2010 budget priorities and the follow-on QHSR mission priorities have served as the basis for annual appropriations requests for four consecutive fiscal years.

I participated in the first review prior to my retirement and we are approaching the second review mandated by the Homeland Security Act. This review presents an opportunity to assess the past ten years and rethink assumptions related to how the broad spectrum of DHS authorities, jurisdictions, capabilities, and competencies should be applied most effectively and efficiently against the risks we are likely to encounter … and how to adapt to those that cannot be predicted, including complex, hybrid events that cross organizational and functional boundaries. This will require a rethinking of what have become traditional concepts associated with homeland security over the last ten years.

Confronting Complexity and Unity of Effort

In 2012 I wrote an editorial for journal Public Administration Review entitled "Confronting Complexity and Leading Unity of Effort." I proposed that the major emerging challenge of public administration and governing is the increased level of complexity we confront in mission operations, execution of government programs, and managing non-routine and crisis events. Driving this complexity are rapid changes in technology, the emergence of global community, and the ever-expanding human-built environment that intersects with the natural environment in new more extreme ways. That environment remains today as we continue to witness extreme weather events, climate change, evolving threats, and the ascendancy of security issues associated with the internet.

The results are more vexing issues or wicked problems we must contend with and a greater frequency of high consequence events. On the other hand advances in computation make it possible to know more and understand more. At the same time structural changes in our economy associated with the transition from a rural agrarian society to a post industrial service/information economy has changed how public programs and services are delivered. No single department, agency, or bureau has the authorizing legislation, appropriation, capability, competency or capacity to address complexity alone. The result is that most government programs or services are "co-produced" by multiple agencies. Many involve the private/non-governmental sector, and, in some cases, international partners. Collaboration, cooperation, the ability to build networks, and partner are emerging as critical organizational and leadership skills. Homeland Security is a complex "system of systems" that interrelates and interacts with virtually every department of government at all levels and the private sector as well. It is integral to the larger national security system. We need the capabilities, capacities and competency to create unity of effort within the Department and across the homeland security enterprise.

Mission Execution … Doing the Right Things Right

As a precursor to the next QHSR there should be a baseline assessment of the current legal authorities, regulatory responsibilities, treaty obligations, and current policy direction (i.e. HSPD/NSPD). I do not believe there has been sufficient visibility provided on the broad spectrum of authorities and responsibilities that moved to the department with the components in 2003, many of which are non discretionary. Given the rush to enact the legislation in 2002 it makes sense to conduct a comprehensive review to validate the current mission sets as established in law.

The next step, in my view, would be to examine the aggregated mission set in the context of the threat environment without regard to current stove piped component activities … to see the department's mission space as a system of systems. In the case of border security/management, for example, a system of systems approach would allow a more expansive description of the activities required to meet our sovereign responsibilities. For the purpose of today's hearing I would like to address four areas: The Border, National Resiliency, Counter Terrorism and Law Enforcement, and Cyber Security.

The Border

Instead of narrowly focusing on specific activities or regions such as the physical security of the Southwest Border we need to shift our thinking to the broader concept of the management of border functions in a global commons. The border has a physical and geographical dimension related to the air, land and sea domains. It also is has a virtual domain where many governmental activities occur such as the processing of advance notice of arrivals, analysis data related to cargoes, passengers, and conveyances, and the facilitation of trade. These latter functions do not occur at a physical border but are a requirement of managing the border in the current global economic system.

The air and maritime domains are different as well. We prescreen passengers at foreign airports and the maritime domain is a collection of jurisdictional bands that extend from the territorial sea to the limits of the exclusive economic zone and beyond. These domains are interconnected and must be seen as a system.

The key concept here is to envision the border as an aggregation of functions across physical and virtual domains instead of the isolated and separate authorities, jurisdictions, capabilities, and competencies of individual components. Further, there are other governmental stakeholders who interests are represented at the border by DHS components (i.e. DOT/Federal Motor Carriers regarding trucking regulations, NOAA/National Marine Fisheries Service regarding the regulation of commercial fishing).

A natural outcome of a functional or systems view of the border is a cause for action to remove organizational barriers to unity of effort, the consolidation of information systems to improve situational awareness and queuing of resources, and integrated/unified operational planning and coordination among components. The additional benefits accrued in increased efficiency and effectiveness become essential in the constrained budget environment. The overarching goal should always be to act with strategic intent through unity of effort. Here the Department continues to be challenged with the internal integration of functions within Customs and Border Protection and the creation of an integrated, fused view of the border across all domains working other components and agencies of government.

Specific areas that would create greater unity of effort and more effective performance include:

- Aggregation of data related to border functions into a single cloud reference architecture (license plate reader data, passenger information, private aircraft and vessel arrivals)
- Sharing and fusing of sensor information across all domains (air, land, sea and cyber)
- Visualization of knowledge through geospatial display tools that allow leaders to see and understand threats
- Addressing issues of border security or control of the border through a functional approach that recognizes the physical diversity border and level of risk by corridors or regions.

National Resiliency

The concept of national resiliency transcends a narrow focus on natural disasters. We need to promote a risk-based whole of community approach that is informed by the collective threat/risks presented by both the natural and human built environments. The latter is a more expansive concept than "infrastructure" and the overall concept subsumes the term "disaster" into larger problem set that we will face. This strategic approach would allow integration of activities and synergies between activities that are currently stove piped within FEMA, NPPD, and other DHS components and other departments of government (i.e. HHS and a pandemic). It also allows cyber security to be addressed as an issue that touches virtually every citizen and player in the homeland security enterprise.

Key components include:

- Regionally based risk assessments that focus on the most likely and consequential threats from the natural and built environments. The latter includes a better understanding of population densities and infrastructure that are exposed to higher risk.
- A better understanding of mitigation and collective action to reduce risks through individual preparedness, local community actions regarding land use and building codes, inclusion of mitigation measures in infrastructure development, better use of scientific data in the understanding and prediction of events, and policies that allocate the cost of risks to those who incur it. The overarching goal is to fundamentally change how risk is viewed by individuals and governments … and to change behavior.
- Development of an improved incident management doctrine that more clearly defines roles and responsibilities and removes ambiguity before, during and after responses. We are seeing more complex events that defy existing response protocols regarding which agency should lead and what roles should other agencies play.
- We need to anticipate hybrid events that cross functional and organizational boundaries. One example of a hybrid event would an man made disaster precipitated by a cyber attack on an industrial control system. Such an event would involve DHS (NPPD, FEMA), the FBI (criminal activity), and potential the defense industrial base. Responding to an event of this nature under current circumstances would be extremely difficult and challenging.
- A national operations center for the Department of Homeland Security that centralizes and visualizes risks and facilitates the monitoring and management of operations. Unity of effort within DHS is the first goal, including greater internal integration in CBP and NPPD.

Counter Terrorism and Law Enforcement Activities

In regard to terrorism and law enforcement operations we should understand that terrorism is, in effect, political criminality and as a continuing criminal enterprise it requires financial resources generated largely through illicit means. All terrorists have to communicate, travel, and spend money, as do all individuals and groups engaged in criminal activities. To be effective in a rapidly changing threat environment where our adversaries can quickly adapt, we must look at cross cutting capabilities that allow enterprise wide success against transnational organized criminal organizations, illicit trafficking, and the movement of funds gained through these activities. As with the "border" we must challenge our existing paradigm regarding "case-based" investigative activities. In my view, the concept of a law enforcement case has been overtaken by the need to understand criminal and terrorist networks as the target. It takes a network to defeat a network. That in turn demands even greater information sharing and exploitation of advances in computation and cloud-based analytics. The traditional concerns of the law enforcement community regarding confidentiality of sources, attribution, and prosecution can and must be addressed, but these are not technology issues … they are cultural, leadership, and policy issues.

Key components include:

- Development and deployment of a classified and unclassified cloud reference architecture that allows the aggregation and analysis of all relevant information held across DHS components including sensor data.
- Development a network discovery doctrine that transitions traditional law enforcement and intelligence "case management" processes to an outcome focused strategy that attacks terrorist and organized crime networks at nodes where they are exposed. This needs to include a more realistic recognition that non-events or the prevention of an attack is preferable, in some cases, to arrest and conviction.
- Aggregation and analysis of biometric information that anticipates advances in technology such as DNA testing and facial recognition that can be readily accessed by field personnel and mobile devices.

Cyber Security

We need to understand that cyber space touches everything and everyone. It is an ubiquitous feature of our lives. Development of better knowledge of this domain in terms of national governance, legal issues and international governance remain works in progress. But the fact is that the internet has produced the sociological, cultural, economic, and legal equivalent of climate change. We must adapt and manage this change. Related to the Department's mission, this includes the protection of the Department's networks, effectively leading the government's protection activities of it's own networks, and, finally, the effective interface with the private sector, state and local governments, and other affected stakeholders to reduce risks and improve national resiliency. These activities must be carried out in cooperation with the Department of Defense, the Intelligence Community, and the Department of Justice to create unity of effort at a national level. There has been recent progress in role definition between these major players. Also, significant activity is currently underway through continuous monitoring initiatives and the presidentially mandated Interagency Task Force to develop a framework to address cyber threats to our critical infrastructure.

Key components include:

- Transition from the current federal information security structure to continuous measurement and mitigation at our internet connections.
- The sharing of information on threats across government and the maturation of information systems and security measures that converge to common architecture

- Development of an effective means to share threat information with the private sector where most of our critical infrastructure resides.
- More effective identification of threats in advance through improved diagnostics
- Cyber legislation to address those areas where administrative action is inadequate to deal with legal issues.

Mission Support

As we address the operational challenges of the Department we must also address the need for improved more integrated mission support. In the rush to establish the Department and in the inelegant way the legacy funding and support structures were thrown together in 2003, it was difficult to link mission execution and mission support across the Department. To this day, most resources and program management of support functions rest in the components. As a result normal mission support functions such as shared services, working capital funds, core financial accounting, human resources, property management, and integrated life cycle based capital investment have been vexing challenges. While this testimony has been focused on operational issues, it is critical that progress be made toward the integration and more effective support of mission execution across the Department.

Conclusion

Mr. Chairman, I have attempted to keep this testimony at a strategic level and focus on thinking about the challenges in terms that transcend individual components, programs, or even the Department itself. I have recently spoken to the Department of Homeland Security Fellows and the first DHS Capstone course for new executives. I have shared many of the thoughts provided today over the last ten years to many similar groups. Lately I have changed my message. After going over the conditions under which the Department was formed and the many challenges that still remain after ten years, I was very frank with both groups. Regardless of the conditions under which the Department was created and notwithstanding the barriers that have existed for ten years, at some point the public has a right to expect that the Department will act on its own to address these issues. Something has to give. In my view, it is the responsibility of the career employees and leaders in the Department to collective recognize and act to meet the promise the Homeland Security Act. That is done through a shared vision translated into strategic intent that is implemented in daily activities from the NAC to the border through the trust and shared values that undergird unity of effort. It is that simple, it is that complex.