Hearing before the House Permanent Select Committee on Intelligence

"Homeland Security and Intelligence: Next Steps in Evolving the Mission"

18 January 2012

American expectations of how their government secures the United States have evolved substantially, especially during the post-9/11 decade. From the post-World War II, 20th-century evolution of the national security architecture in the United States, focused on countering overseas nation-states with conventional forces, we now face requirements to protect at home. And not only to protect, but to prevent: the new, domestic security architecture is targeted more at securing borders, infrastructure, and cyberspace with defensive measures as it is at pursuing any single adversary with offensive measures.

The growth of our expectations of domestic security, and the evolution of threats away from traditional state actors toward non-state entities -- drug cartels, organized crime, and terrorism are prominent examples -- suggest that the DHS intelligence mission should be threat agnostic. Though the impetus for creating this new agency, in the wake of the 9/11 attacks, was clearly terrorism-based, the kinds of tools now deployed, from border security to cyber protection, are equally critical in fights against emerging adversaries.

The DHS enterprise is more complex than other agencies responsible for America's security, and its intelligence mission is correspondingly multifaceted. Its intelligence missions range from providing homeland security-specific intelligence at the federal level; integrating intelligence vertically through DHS elements; and working with state/local/private sector partners to draw their intelligence capabilities into a national picture and provide them with information. DHS, as it works to sharpen these missions, benefits from both a legislative mandate and a competitive advantage in a few areas that are unique within the federal intelligence community:

- Securing borders and analyzing travel -- from threats such as terrorists, drug cartels, and alien smugglers -- including integrating travel data with other federal information;
- Protecting critical infrastructure, from advising transportation partners on how to secure new transport nodes to providing sectors with after-action analysis of the infrastructure vulnerabilities exposed by overseas attacks; and
- Preventing cyber intrusions, from red-teaming vulnerabilities in the US private sector to sharing best practices among corporate entities.

Many agencies conduct all-source analysis of threat based on more traditional models of intelligence. As DHS grows its intelligence mission, though, we should understand that its development will benefit from unique data and responsibilities that other agencies do not share. The foundation for a separate DHS intelligence mission includes a few key elements:

- Access to unique, homeland-relevant data, such as CPB and ICE information;
- Responsibility for securing the border and critical infrastructure;
- Access to personnel who have intimate tactical knowledge of current issues and trends in these areas; and
- Responsibility for serving state/local partners as well as private sector partners in key infrastructure sectors.

In an age of budget constraints, pressure on DHS to focus on core areas of responsibility and capability -- and to avoid emphasis on areas performed by other entities -- may allow for greater focus on these areas of core competency while the agency sheds intelligence functions less central to the DHS mission. Analysts and managers in Washington's sprawling intelligence architecture often

speak of the value of competitive analysis -- analysts at different agencies, for example, looking at similar problems to ensure that we miss no new perspective, no potentially valuable data source.

There remains room for this type of analysis, but there are enough agencies pursuing the terrorist adversary to allow DHS to build a new analytic foundation that emphasizes data, analytic questions, and customer groups that are not the focus for other agencies. Analysis that helps private-sector partners better understand how to mitigate threats to infrastructure, for example, should win more resourcing than a focus on all-source analysis of general threats, such as work on assessing the perpetrators of attacks. Conversely, all-source analysis of terrorist groups and general terrorist trends should remain the domain of other intelligence agencies.

In contrast to intelligence agencies that have responsibilities for more traditional areas of national security, DHS's mandate should allow for collection, dissemination, and analytic work that is focused on more specific homeward-focused areas. First, the intelligence mission could be directed toward areas where DHS has inherent strengths and unique value (e.g., where its personnel and data are centered) that overlap with its legislative mandate. Second, this mission direction should emphasize areas that are not served by other agencies, particularly state/local partners whose needs are not a primary focus for any other federal agency.

In all these domains, public and private, DHS customers will require information with limited classification; in contrast to most other federal intelligence entities, DHS should focus on products that start at lower classification levels, especially unclassified and FOUO, and that can be disseminated by means almost unknown in the federal intelligence community (phone trees, Blackberries, etc.).

Partnerships and collaboration will be a determining factor in whether this refined mission succeeds. As threat grows more localized, the prospect that a state/local partner will generate the first lead to help understand a new threat, or even an emerging cell, will grow. And the federal government's need to train, and even staff, local agencies, such as major city police departments, will grow. Because major cities are the focus for threat, these urban areas also will become the sources of intelligence that will help understand these threats at the national level, DHS might move toward decentralizing more of its analytic workforce to partner with state/local agencies in the collection and dissemination of intelligence from the local level.

This new approach to intelligence -- serving local partners' requirements, providing intelligence in areas (such as infrastructure) not previously served by intelligence agencies, and disseminating information by new means -- reflects a transition in how Americans perceive national security. For this reason, state/local agencies, as clients for DHS intelligence, should also be involved in the development of requirements for what kinds of intelligence on emerging threats would be most helpful, from changing tactics for smuggling aliens into the United States to how to understand overseas terrorist incidents and translate them into analysis for the US.

Similarly, different private sectors in the United States, from the hospitality industry to transportation, should drive requirements for DHS, in addition to serving as sources for information about what emerging vulnerabilities these industries are seeing. DHS should utilize existing public private partnerships to both drive requirements and aid distribution.

After the Mumbai attacks, for example, DHS intelligence might have partnered with private sector entities in the hospitality industries -- and state and local police agencies responsible for major hotel centers and ports -- to develop unclassified graphics and text explaining how the terrorists entered ports; how they breached perimeter security at facilities in the city; how security within facilities struggled during the ensuing battle; and how the attacks compared with other attacks in recent years against public buildings. Most or all of this information would have been available in public media, and it can be displayed in interactive, graphic format, with support from analysts who specialize not in international terrorism but instead in engineering, building security, port security, etc. The requirements for any product would have been driven by the hospitality industry and major city police chiefs. None of this bears any resemblance to what more traditional intelligence agencies have done since in post-WWII world of foreign intelligence; this type of analytic product is more closely aligned with the new, and growing, world of homeland security intelligence.

By focusing intelligence collection, dissemination, and analysis in these areas, DHS could grow an intelligence architecture that builds on its core strengths, avoid competition with agencies in other areas, such as general terrorism analysis; and provide unique product and partnerships that other agencies not only lack but are will not view as their core competencies.

Because homeland security intelligence requires a new understanding of products, customers, and delivery, training managers and analysts must reflect a way of doing business that is fundamentally different than the business practices taught at agencies that have focused historically on foreign intelligence. DHS might consider the development of a homeland security training institute that develops this training -- from new ways to portray information geospatially to different paths for developing requirements from state and local partners -- as an entirely new enterprise. This training

should include a separate element responsible for research, for bringing in American and foreign scholars who look at this issue, and for ensuring that doctrines for collecting, reporting, and analyzing knowledge in the homeland security environment is captured in one place and documented.

The creation of DHS led to a rapid growth in a workforce, and a thirst for analytic product, that required the US Government to move quickly, before the foundations of homeland security intelligence were established and before we had the luxury of a full post-9/11 decade to understand where we need to go. We have an opportunity now to step back and review how much this new enterprise differs from traditional analysis, and how we can succeed, beyond what we understood even five years ago, in delivering new, innovative product to different customers. And in how we can develop simple processes through which they deliver clear requirements to analysts in Washington and at fusion centers across the country. This review provides that opportunity.