Hearing before the House Permanent Select Committee on Intelligence

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

Statement for the Record

Philip Mudd
Member, Aspen Homeland Security Group
Former Deputy Director of National Security
Federal Bureau of Investigation
Former Deputy Director, Counterterrorist Center
Central Intelligence Agency

18 January 2012

More than a decade after 9/11 and years after the establishment of the Department of Homeland Security (DHS), the Aspen Institute has drawn together a broad spectrum of senior experts to study how the Department's unique intelligence program might continue to evolve. Changes in how Americans view national security have served as the backdrop: America's post-WWII security focus centered on overseas threats, but we now know that national security involves state and local police; border security; transportation and other infrastructure; and many other public- and private-sector entities that are new to our understanding of how national security should work.

To reflect the globalization of threat, from cartels and gangs in Latin America to terrorism, child pornography, human trafficking, and other transnational problems, we need a new approach to homeland intelligence. This approach should serve local partners' requirements, providing intelligence in areas (such as infrastructure) not previously served by federal intelligence agencies, and disseminating information by new means such as smartphones.

- These changing threats suggest a threat-agnostic service: with more established threats from drug cartels and terrorists, to new cyber problems, DHS's analytic mission should not focus primarily on terrorism.

DHS has multiple missions: 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 threat 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. None combine DHS's characteristics, including 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. Analysis that helps private-sector partners understand how to mitigate infrastructure threats, for example, might merit more resources than all-source

analysis of general threats. 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. And in all these domains, the starting point should be unclassified information that can be shared readily.

Partnerships and collaboration will be a determining factor in whether this refined mission succeeds. As threat grows more local, the prospect that a state/local partner will generate the first lead to help understand a new threat will grow. And the federal government's need to train, and even help 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 intelligence sources driving an understanding of these threats at the national level. As a result, 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.

State/local agencies and private sector partners, as clients for DHS intelligence, should also be involved in developing requirements for what intelligence on emerging threats would be most helpful, from changing smuggling tactics to how to understand overseas terrorist incidents and translate them into analysis for the US.