

**United States Department of Homeland Security
Office of Intelligence and Analysis**

**Statement for the Record
Caryn A. Wagner
Under Secretary and Chief Intelligence Officer**

**Before the
House Committee on Homeland Security
Subcommittee on
Intelligence, Information Sharing, and Terrorism Risk Assessment
United States House of Representatives**

September 29, 2010

Introduction

Chairman Harman, Ranking Member McCaul, and distinguished Members of the Subcommittee, thank you for the opportunity to appear before you today to discuss how the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) interfaces, supports and coordinates with headquarters elements of the Department – the offices and directorates at the headquarters level that report directly to the Secretary, outside of our seven operating components.

Before I address the main topic of this hearing, I must echo the Secretary's testimony from September 22, 2010: the terrorist threat to our country is changing in ways that increasingly challenge law enforcement and the Intelligence Community. The Department is moving at all levels to address this evolving threat; preventing terrorist attacks in today's dynamic threat environment means working in a unified way across all levels of government. DHS' intelligence mission, which I am honored to lead, is to sustain a unified and synchronized Intelligence Enterprise that enables informed decision-making at DHS and in the entire homeland security enterprise. The mission of I&A is to strengthen the Department's and our partners' ability to perform their homeland security functions by accessing, integrating, analyzing and sharing timely and relevant intelligence and information, while protecting privacy and civil liberties.

The Office of Intelligence and Analysis Strategic Vision

I&A is charged with leading the Department's efforts to provide intelligence and information in a useful form to departmental decision makers, headquarters and operational components, state, local, tribal and private sector partners, and the national Intelligence Community. Our job is to serve as the two-way conduit for information that supports protecting the homeland. I&A's programs, projects and activities align with the core DHS missions designated in the Quadrennial Homeland Security Review (QHSR). To that end, I&A plays a critical role to DHS' success in all of its core mission areas: preventing terrorism and enhancing security, securing and managing our borders, enforcing and administering our immigration laws, safeguarding and securing cyberspace, ensuring resilience to disasters, and strengthening and maturing the Department.

In my last appearance before this Subcommittee in May, I addressed the evolution of the DHS Intelligence Enterprise and how it interacts with departmental operational components. Today, I appear before you to discuss the ways in which I&A supports the headquarters elements of the Department.

Intelligence Support to DHS Headquarters Elements

A key reason for I&A's existence is to support the intelligence needs of the Department as a whole. To this end, I firmly believe that I&A must provide the entire Department with a common understanding of the threat. In ascribing to this model, I am dedicated to providing timely, relevant and vigorous intelligence support to DHS headquarters

elements, as well as to the Department's operational components. This, of course, is in addition to our focus on supporting the intelligence and information sharing needs of our non-federal partners, the national Intelligence Community, and the nation's private sector.

I&A interacts with headquarters elements within DHS in accordance with the authorities given to me as the Department's Chief Intelligence Officer. This interaction includes I&A production of analytic products tailored to the needs of DHS headquarters elements. I use my dual authority, as both the Under Secretary and Chief Intelligence Officer, to ensure that Department investments in intelligence programs, projects and activities are focused on departmental and national priorities, closing gaps, eliminating redundancies, and ensuring that investments in intelligence are measured for utility and outcome.

I&A supports, interacts and shares information with DHS headquarters elements in many ways. These include the following elements:

Science and Technology Directorate (S&T)

S&T is one of I&A's principal departmental customers. I&A provides monthly and ad hoc intelligence briefings to Dr. Tara O'Toole, the DHS Under Secretary for Science and Technology. These customized briefings are designed to meet her intelligence needs. I&A disseminates finished intelligence assessments to specific customers in S&T on a regular basis, and interacts with decision making and subject matter expert counterparts at least several times a week. I&A participates in and manages Intelligence Community input to the threat elicitation phase of S&T's Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism Risk Assessments, including the Bioterrorism Risk Assessment, and the Integrated CBRN Terrorism Risk Assessment for the Department.

I&A plays a significant role in supporting the Material Threat Assessments, which were developed by S&T to support the Secretary in issuing Material Threat Determinations pursuant to the *Project Bioshield Act of 2004*. Members of I&A also serve on the Biodefense Knowledge Center Advisory Board and the National Biodefense Analysis and Countermeasures Center Science Advisory Board.

National Protection and Programs Directorate (NPPD)

I&A has a unique, ingrained relationship with the DHS Office of Infrastructure Protection (IP), which resides in NPPD. As you know, I&A's precursor organization combined the missions of intelligence and analysis with infrastructure protection. Today, I&A provides enduring support through its participation in the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), a departmental fusion center designed to facilitate the sharing of threat and risk information with IP's public and private sector partners in the nation's critical infrastructure community. I&A also collaborates closely with NPPD's cybersecurity elements, including the United States Computer Emergency Readiness Team (U.S.-CERT).

Support to Infrastructure Protection

Through analysts assigned to HITRAC, I&A has provided regular, steady-state and incident-specific classified and unclassified briefings and reports to federal, state, local, and private sector critical infrastructure protection community members; supported the development of the annual National Risk Profile included in the congressionally required National Critical Infrastructure and Key Resources (CIKR) Protection Annual Report; and participated in exercises designed to improve public and private sector responses to current and emerging threats to critical infrastructure. Recent examples include supporting the July 2010 tabletop exercise on reducing the vulnerability of the U.S. food supply to intentional contamination and subsequent Infrastructure Protection Note, as well as a May 2010 five-city classified briefing series on the nation's evolving threat picture to state and local critical infrastructure partners.

I&A further supports IP's efforts to build critical infrastructure expertise in state and local fusion centers. For example, I&A and IP are jointly conducting a training course for state and local fusion center infrastructure analysts to provide them with an overview of risk analysis tradecraft, including threats to critical infrastructure. I&A and IP are also collaborating to support an exchange program that brings state and local fusion center infrastructure analysts to Washington, D.C. for threat briefings and training – an iteration of this program is occurring this week. Most recently, I&A and IP held a joint annual meeting for I&A's fusion center analysts and IP's field-deployed Protective Security Advisors to facilitate collaboration and mutual awareness.

I&A and IP work together on additional specialized projects and programs. For example, they are collaboratively developing infrastructure sector-specific intelligence requirements and a comprehensive information requirements process, which will further improve the ability of I&A and the Intelligence Community to meet the information needs of the nation's critical infrastructure community. I&A works closely with IP's Office for Bombing Prevention (OBP) on issues related to improvised explosive devices and chemical, biological, radiological and nuclear (CBRN) and explosive threats, and supports IP's operational programs such as Enhanced Critical Infrastructure Protection security surveys at critical infrastructure facilities and the Regional Resiliency Assessment Program. I&A reviews and provides substantive comments on information reports derived from OBP's Technical Resource for Incident Prevention (TRIP*wire*), which describe terrorist use of bombs and Improvised Explosive Devices. I&A products are frequently posted on the TRIP*wire* portal for use by applicable stakeholders.

Support to Cybersecurity

I&A provides substantial and growing support to the cybersecurity and protection activities of the Department. This support includes tactical and strategic threat intelligence analysis for elements of NPPD's Office of Cybersecurity and Communications. I&A delivers tactical intelligence support – situational awareness and early warnings of potential cyber threats that combine all-source analysis with data from EINSTEIN sensors – to the National Cybersecurity and Communications Center

(NCCIC), US-CERT, the National Coordinating Center for Telecommunications (NCC), and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). I&A publishes Homeland Information Reports derived from intrusion or other exploited cyber data, which identifies cyber-focused collection gaps and generates requirements based on these gaps. I&A further develops and delivers strategic intelligence products and services, such as assessments, briefings and teleconference support, to numerous customers, including CIKR customers through Sector Coordinating Councils (SCC), Government Coordinating Councils (GCC), and state and local government authorities. These products can relate to cybersecurity or physical cyber-related infrastructure.

Office of Operations Coordination and Planning (OPS)

I&A has a mutually reinforcing relationship with OPS; I&A is the Department's primary intelligence element and OPS is responsible for maintaining full awareness of all DHS activities and relevant developments. I&A's primary support to OPS is in providing needed intelligence and information to the National Operations Center (NOC). I&A maintains an embedded classified-level watch and warning function at the NOC that serves as the immediate conduit for intelligence and information obtained from I&A's myriad customers.

I&A coordinates with OPS to address requirements for the Department's Single Point of Service (SPS) program. This program, consisting of elements from the NOC, I&A, and the DHS Office of Intergovernmental Affairs, processes support requests in a visible, transparent and accountable manner. Support requests include requests from state, local, tribal and territorial partners for support to include Requests for Information, classification downgrades, on-site training, and briefing support. I&A ensures that support requests forwarded by the NOC conform to I&A's authorized missions, qualitative standards, and legal and regulatory requirements; protect individual privacy, civil rights, and civil liberties; are responsive to the requirements of I&A customers; and maintain the integrity of the departmental intelligence process.

I&A directly supports OPS via its embedded Operations Intelligence staff. For example, our health intelligence team supported OPS' H1N1 Operations Planning Team during the H1N1 pandemic. More recently, I&A's Operations Intelligence staff and chemical and biological threats analysts were fully integrated into developing and implementing departmental CBRN and health response plans. This was done in close tandem with OPS and other Department elements and components.

Even though the DHS Chief Intelligence Officer is the head of the Department's statutory program to support state and local fusion centers, OPS, mainly through the NOC, has key responsibilities in furthering the Department's commitment to sustain and support fusion centers. I&A appropriately coordinates with OPS in salient areas such as fulfilling support requests received from fusion centers.

Domestic Nuclear Detection Office (DNDO)

I&A provides strategic intelligence assessments that focus on threat actors, their claims, and their plans to attack the United States with radiological and nuclear materials. These assessments support DNDO's policymaking and resource planning efforts. In addition, I&A produces baseline and estimative intelligence products to enable Global Nuclear Detection Architecture (GNDA) planners to anticipate adversaries' future capabilities and intent and develop a better understanding of the future environment in which the GNDA will operate. I&A products support DNDO as the departmental lead in developing the GNDA, which includes red teaming and reviewing deployment strategies.

Office of Health Affairs (OHA)

I&A's partnership with OHA entails close collaboration at multiple levels. I&A provides tailored monthly briefings for Assistant Secretary and Chief Medical Officer Dr. Alexander Garza to address his key intelligence questions. I&A produces intelligence analysis to meet OHA's unique information needs; for example, I&A recently provided tailored analysis and briefings to support OHA's BioWatch Program. I&A coordinates with OHA to provide the Secretary, DHS elements and components, and state, local, tribal, territorial and private sector customers with appropriate products that detail CBRN and health intelligence threat assessments, as well as related medical countermeasures and infectious disease mitigation techniques.

I&A and OHA collaborate closely on the Health Security Intelligence Enterprise (HSIE), a joint initiative to integrate the public health and healthcare communities into the Department's intelligence and information sharing programs and processes. The HSIE focuses on building multidisciplinary partnerships to facilitate a two-way flow of information among state and local health officials and the national network of state and local fusion centers. The ongoing collaboration and coordination for the HSIE initiative represents a valuable partnership between I&A and OHA.

On the programmatic front, I&A coordinates with the National Biosurveillance Integration Center (NBIC) on a regular basis, participating in its daily biosurveillance teleconferences, providing salient finished intelligence products, and responding to NBIC's requests for information on disease events around the world. As part of this partnership, I&A provided the medical intelligence briefing for the inaugural Food Protection Workshop that NBIC cosponsored with the federal Food Safety and Inspection Service (U.S. Department of Agriculture) this summer.

Office of Policy

I&A provides distinct intelligence support to DHS' Office of Policy in ensuring that its decisions and initiatives are informed by the latest intelligence and threat analysis. This includes focused support on counter-terrorism, watch-listing and screening, national and international information sharing access agreements, departmental strategic planning and risk management, and preventing the unauthorized acquisition or use of CBRN materials and capabilities. For example, we provided intelligence that supported Policy's

involvement in the implementation of Executive Order 13546, “Optimizing the Security of Biological Select Agents and Toxins in the United States.”

Multiple I&A divisions, including its Strategies, Plans and Policy Division, Information Sharing and Intelligence Management Division and its Border Security Division, work in close collaboration and cooperation with various elements within the Office of Policy. These engagements ensure that the decisions and initiatives of sub-offices within Policy are informed by the latest intelligence.

Our program and intelligence analysts coordinate with the Office of Policy in addressing intelligence requirements for the Visa Waiver Program. Using the mandate from the 9/11 Act, the Director of National Intelligence designated DHS as the lead Intelligence Community entity responsible for biennial Visa Waiver Program assessments. We independently assess the integrity and security of travel processes and documentation for each country in or applying to the program to address the potential for illicit actors—including transnational criminals, extremists and terrorists—to exploit travel systems and the security environment that can facilitate unlawful access to the United States.

I&A, as the statutory lead for establishing intelligence policy for the Department’s Intelligence Enterprise, ensures appropriate coordination with the Office of Policy in all our intelligence and information sharing activities. I&A provides direct intelligence policy input to the formulation of Office of Policy strategies and initiatives, such as those associated with our Southern and Northern borders, counterterrorism, screening coordination, and information sharing with U.S. and international partners.

Office of Security

I&A provides significant support to the Office of the Chief Security Officer on a variety of issues, including the development of implementation guidelines for Executive Orders impacting classified information management. Other pertinent collaborative activities include the issuance of security clearances to non-federal partners and building and accrediting Sensitive Compartmented Information Facilities, or SCIFs.

Office of Counternarcotics Enforcement (CNE)

I&A provides CNE with analytic and intelligence support for its efforts to coordinate DHS responsibilities to stop the entry of illegal drugs into the United States, and track and sever the connections between drug trafficking and terrorism. I&A is a member of the CNE-led Counternarcotics Coordinating Council, a body that coordinates Department counternarcotics policy and operations.

I&A provides substantial support to the development of national and DHS counternarcotics strategies. Significantly, I&A served as a co-chair, along with the U.S. Drug Enforcement Administration, of the interagency effort to develop the intelligence and information sharing chapter in the 2009 *National Southwest Border Counternarcotics Strategy*. I&A is responsible for tracking over 100 such interagency initiatives alongside

CNE, and is currently assisting CNE in the development of a DHS strategy to combat the links between drug trafficking and terrorism.

I&A supports CNE with subject matter expertise on drug trafficking trends along our Northern and Southern borders, serving as CNE's link to the Intelligence Community for obtaining information and intelligence on the threats posed by international drug trafficking and on the connections between drug trafficking and terrorism. I&A works closely with CNE to ensure that its information needs are incorporated into the DHS Standing Information Needs (SINs). DHS SINs identify the universe of enduring intelligence needs of the Department, and allow the DHS Chief Intelligence Officer to focus collection, analytic and reporting activities and efforts based on the distinct needs of the Department and its customers. I&A also facilitates CNE's requests for information to the Intelligence Community on international drug trafficking and drug-terror nexus issues.

Other Areas of Interaction with DHS Headquarters Elements

National Security Systems

I&A management of the DHS National Security Systems (NSS) Program provides a significant enabling capability to departmental decision makers, including in headquarters elements. The NSS is a joint initiative between I&A and the Office of the Chief Information Officer (OCIO). The Deputy Secretary chartered the NSS in January 2009 to bring a One DHS approach to the management of all classified information technology infrastructure provided by DHS, including networks, secure communications and enterprise services. This joint initiative institutionalizes a strong mission partnership between OCIO and I&A in the relatively small and specialized – but critical – area of classified information technology capability.

The NSS Program provides clear benefit for DHS headquarters elements, as well as operational components, to ensure their users have appropriate access to classified information technology infrastructure, such as the Homeland Secure Data Network. These benefits include consolidated, enterprise-level management of all classified information technology services; strengthened alignment to departmental and component mission priorities; coordinated investments for efficiency and interoperability; and improved service delivery and transparency.

Intelligence Training

I&A supports DHS headquarters elements by offering many intelligence tradecraft and other related training multiple times each year. Intelligence training is a critical capability that enables fulfillment of the Department's intelligence mission. We are building on existing intelligence training successes and expanding this program to establish a culture of disciplined and uniform intelligence capabilities throughout the Department. Strong intelligence tradecraft across the Department serves the dual purpose of making headquarters consumers of intelligence more informed of what intelligence can – and cannot – provide to DHS decision makers.

Strengthening Interface

In preparing for this hearing, I identified several areas in which I&A can improve its support to DHS headquarters elements. We are making strides in how we provide the Secretary and Deputy Secretary tailored and timely all-source intelligence briefings. We have engaged key decision makers across the Department and asked them how I&A can better fulfill their requirements. I have found the feedback from these inquiries to be both helpful and substantive.

I&A has used this feedback to accelerate understanding of departmental policy deliberations and the programmatic activities of DHS headquarters elements. Stronger insight by I&A into departmental policy and programmatic matters will make us more attuned to the needs of our customers, and thus more focused on the core intelligence questions and needs of DHS decision makers.

Conclusion

Members of the Subcommittee, I appreciate the opportunity to appear before you today to discuss how I&A supports and coordinates with headquarters elements within the Department. I&A has made significant strides, and continues to adapt to the current and emerging needs of our partners and customers across the Department. I&A has a vital and unique mission and continues to improve its strategic posture to more effectively support core customers, including DHS headquarters elements.

I&A's efforts to manage, collect, analyze and share intelligence and information will continue to be guided by the dual imperatives of protecting the country from those who wish to do us harm, and protecting the privacy, civil rights, and civil liberties of our citizens. With your support, the leadership of Secretary Napolitano, and the fine men and women of I&A, I believe we can accomplish our multi-faceted mission and help DHS headquarters elements accomplish theirs. I look forward to keeping the Subcommittee and Congress apprised of I&A's continued progress in this important area, as well as our progress in leading and strengthening the critical intelligence mission of the Department.

Thank you for your time, and I look forward to your questions.

###