

Keynote Address at National Homeland Defense Foundation by Charles E. Allen, Under Secretary for Intelligence and Analysis/Chief Intelligence Officer



Release Date: October 30, 2008

Colorado Springs, Colo.
National Homeland Defense Foundation

Introduction

I am delighted to be here in Colorado to address this sixth annual Symposium of the National Homeland Defense Foundation. I would like to thank my friend John Gannon for inviting me to share with you the progress of DHS' efforts to secure the Homeland and to describe the many ways DHS works in collaboration with partners at home and abroad. The Foundation's efforts in bringing all of us together to discuss how we can all perform our missions better should be lauded. Some people believe that because we have managed to go over seven years without an attack on the Homeland, the urgency of homeland defense and homeland security is not as high a priority. But as you know, it is no accident that we have not suffered a major terrorist attack on U.S. soil since September 11, 2001. It is the result of the hard work and constant vigilance of hundreds of thousands of men and women – including DHS employees, and our many partners here and abroad – who are working tirelessly to protect our country. As Mike Hayden has stated publicly, we are "playing offense."

We must recognize that the United States continues to face serious threats. We recognize that the threats facing the United States today are more complicated, transcend international borders, and evolve more rapidly than ever before. Most immediately, this country remains engaged in a long and sustained struggle against the violent, ideological extremism of al'Qaida's core leadership, its affiliated extremist networks, and a growing number of followers who are self-radicalized. And, in a highly globalized world, distant threats can rapidly manifest themselves at our borders. As the unclassified key judgments of the July 2007 NIE points out—we are in a period of sustained strategic warning.

But terrorism is not the only threat we face. Drug traffickers and alien smugglers attempt to evade our border security procedures daily. We remain on guard against Latin American drug trafficking organizations – with the ability to penetrate successfully our borders using extensive logistics networks – that might support such a terrorist undertaking. Within the United States we also face the danger of domestic extremists from across the spectrum of ideological beliefs: white supremacists; Islamic radicals; eco-terrorists; animal rights extremists; and anarchists all have the potential to conduct violent attacks. Because of this diverse threat landscape, our Department's analytical and operational efforts are focused on all-threats—not just terrorism. Secretary Chertoff defines the Department's mission as keeping out dangerous people and dangerous goods and protecting our critical infrastructures.

But we realize we are not in this fight alone. Last month, at the request of Secretary Chertoff, the Homeland Security Advisory Council, or HSAC, provided a list of the top ten challenges facing the next Secretary of the Department. What was the first Key Challenge identified by the HSAC? Understanding that *"homeland security is more than just a single cabinet department."* The HSAC reported that: "The Department of Homeland Security is unique in government in its complex need for both horizontal and vertical integration with other organizations and groups." The report goes on to state that, "Securing the homeland requires sharing responsibility horizontally with other Federal departments and agencies," as well as vertically to achieve a "robust...integration of the federal, state, local, and tribal governments, the private and non-profit sectors, and the American citizen to build a secure, safe, and resilient Nation." I could not agree more. More simply put: to accomplish its mission, the Department of Homeland Security **must** collaborate with partners at all levels of government at home and abroad.

As you know, the Intelligence Community's focus traditionally has been aimed at foreign threats and its customer set focused on international level partners. The Community's interaction with State, local and tribal law enforcement and other first responders intentionally was limited or non-existent. But homeland security, in a post-9/11 world, requires a new paradigm for intelligence support. This shift has led to a new information sharing landscape – one including new partners, new roles, and new rules that are still evolving. DHS is squarely at the

center of this new paradigm.

The DHS Intelligence Mission

My task as Under Secretary for Intelligence and Analysis and the Chief Intelligence Officer for the Department has been to lead the effort to develop the vision for, design the architecture of, and implement a comprehensive homeland security intelligence program that is **fully integrated** into the traditional Intelligence Community but which **equally** reaches out to new, essential partners at all levels of government.

This has been no small task and has required new authorities, new structures, and new kinds of cooperation across the Community. DHS intelligence authorities were first established in the *Homeland Security Act of 2002*, with additional authorities provided later in the *Intelligence Reform and Terrorism Prevention Act of 2004*, and the *Implementing Recommendations of the 9/11 Commission Act of 2007*. The specific mission of the Office of Intelligence and Analysis, or I&A—DHS' primary representative in the Intelligence Community—was most recently enhanced by the amendments to Executive Order 12333.

Ever since I arrived at DHS in late 2005, I have been committed to delivering results against the critical mission priorities identified by the Secretary. I am consistently amazed by the breadth of the customer set we serve. It is unique in the Intelligence Community. The DHS Intelligence Enterprise – Department components with dedicated intelligence functions - must effectively serve all homeland security customers, including all of DHS, our State, local, tribal, territorial, and private sector partners, the Intelligence Community, and our international partners. Each of these customers has different needs.

Let me put this in perspective by giving you an idea of the scope of DHS' activities that DHS Intelligence must support **every single day**—consider this:

- Customs and Border Protection processes more than a million passengers and pedestrians, 70,000 containers, and more than 300,000 air, sea, or land vehicles.
- The Transportation Security Administration screens 2 million passengers and nearly as many pieces of checked luggage before they board commercial aircraft.
- Citizenship and Immigration Services conducts an average 135,000 national security background checks, and adjudicates an average of 200 refugee applications.

As for enforcement activities, DHS carries out **each day**:

- CBP apprehends an average of 2,400 people crossing illegally into the United States. Some are individuals of special interest to the United States and our job is to ensure they are interviewed and we harvest the intelligence information these people possess.
- TSA intercepts nearly 18,000 prohibited items at checkpoints, including almost 3,000 knives and 200 other dangerous items.
- The U.S. Coast Guard interdicts an average of 17 illegal migrants at sea, and seizes an average of 1,000 pounds of illegal drugs worth nearly \$13 million.

DHS' Intelligence primary customer is the Department—including both headquarters as well as operational components. The incredibly broad DHS mission requires having reliable, real-time information and intelligence to allow the Department to identify and characterize threats uniformly, support security countermeasures, and achieve unity of effort in the response.

An equally important customer is our State and local partners. As I will describe in more detail later, we are ensuring these stakeholders have access to our key intelligence and information capabilities, and the Department, in turn, has access to information obtained by these partners in the course of their operations.

In addition, DHS Intelligence and Analysis is reaching out to a broad spectrum of private sector representatives. We have learned that private sector information requirements are not only numerous, but have become more complex as our private sector partners have become more knowledgeable about our capabilities to support them.

As a result we have focused products and services to meet these particular needs. I know you have already heard from Jim Caverly about the broader DHS efforts to protect critical infrastructures, most of which are in the private sector.

Finally, the Intelligence Community remains an important customer. My Office is a member of the Intelligence Community, under the leadership of the Director of National Intelligence. It is taking its place in senior Intelligence Community forums, including serving as a member of the DNI's Executive Committee. We are also participants in implementing the DNI's *National Intelligence Strategy* and *500-Day Plan*; the landmark theme of both is collaboration among IC members.

International Collaboration

Although collaboration with foreign partners is nothing new for the Intelligence Community, I am constantly struck by how the United States is cooperating even more closely with other countries to prevent terrorism and other significant threats from harming the Homeland. DHS is committed to strengthening our international ties and working together through intelligence and information sharing, and in some cases coordinated operations with foreign partners. We recognize that strengthening bonds with our allies is one of the most important steps our country can take to ensure lasting security. And as a newer member of the Community, DHS Intelligence is developing new ways to collaborate with these critical partners.

To see concrete benefits of these collaborative efforts we need only to look to DHS' response during the disruption of the plot in the UK, two summers ago, to destroy American commercial airliners bound for the United States. To foster this type of international collaboration, in 2003 we established with our British partners the Joint Contact Group, or JCG, that is co-chaired by DHS' Deputy Secretary and the U.K. Permanent Home Secretary. This Group provides strategic direction and cooperation for joint U.S. – U.K. homeland security efforts, on areas such as encouraging the division of labor between the two countries on homeland security projects; serving as a venue for the exchange of lessons learned and security experiences; and promoting joint participation in homeland security exercises. The JCG promotes an interpersonal environment, which made international collaboration easier while addressing such a highly sensitive threat as the airliner plot.

One of the main lessons of the 9/11 attacks, and subsequent attacks in Europe and elsewhere, is that we must shatter barriers to information sharing, including with our international partners. In the recent changes to Executive Order 12333, the DHS Under Secretary for Intelligence and Analysis is mandated to share intelligence and information with foreign governments under approved agreements. My Office is now authorized to participate in information and analytical exchanges with foreign partners. To show our dedication to international intelligence collaboration, I have established a foreign disclosure office. This unit facilitates sharing of intelligence and information with our international partners by serving as a two-way conduit for foreign governments to ask for and appropriately receive intelligence and information from DHS, and vice versa. All the while, we coordinate with the DNI and CIA as appropriate and necessary.

My Office interacts regularly with traditional allies such as the United Kingdom, Canada, New Zealand, and Australia to share appropriately threat information and intelligence. We are developing cooperative relationships with Mexico and several other European and Asian countries as well. Common topics of discussion include protection of critical infrastructure, study of radicalization and extremism, and border security. In addition, we have published joint assessments with counterpart agencies in Europe and elsewhere.

An extremely important international information sharing initiative, led by DHS, covers air passengers traveling between partner countries and the United States. Passenger Name Record, or PNR, data, allow DHS' inspection officers to check passenger names and other basic information against lists of known or suspected terrorists and criminals before they board the aircraft so people we will not allow into the country cannot even get on the plane. The ability to identify subtle links between passengers and known dangerous people has made PNR data invaluable to our counterterrorism efforts.

But obtaining timely and accurate PNR data is not possible without the robust involvement of our international partners. In July 2007, the European Union and the United States signed an agreement, applicable for seven years, on the processing and transfer of PNR data by foreign air carriers to DHS. In return, DHS guarantees a significant level of privacy and security protections for the data it receives.

DHS now receives PNR data before the scheduled airline departure. DHS can subsequently transmit the data to U.S. authorities responsible for law enforcement, public security or counterterrorism. DHS also transmits analytic data flowing from PNR data to partner European authorities.

I do not know how many people know this, but post-attack analysis using PNR data on the September 11 hijackers linked all 19 perpetrators. Just think if we had this tool available prior to 9/11. PNR is a valuable counterterrorism tool that needs to be expanded to permit DHS to fully leverage this important information sharing and analysis mechanism, while always remaining sensitive to foreign government privacy concerns in the handling of the data.

We have also seen progress this year pertaining to our Visa Waiver Program. For more than a generation, this program has allowed visitors from certain countries to enter the United States without first obtaining visas. To expand the program, DHS has signed memoranda of understanding with eight nations that aspired to join the program – Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, the Republic of Korea, and Slovakia. These memoranda of understanding require, among other things, that both countries enhance information sharing on international travel and border screening, improve information exchanges on known and suspected terrorists, and provide timely and comprehensive reporting of lost and stolen passports. This paves the way not only for enhanced commerce, but for expanded information sharing, wider use of air marshals, and safer airports.

As a result of the 9/11 Act, the DNI designated my Office as the Intelligence Community's entity responsible for independently assessing the integrity and security of travel processes and documentation for each country in or applying to the program. These assessments address the potential for illicit actors—transnational criminals, extremists, and terrorists—to exploit travel systems and security vulnerabilities in order to facilitate unlawful access to the United States. To date, we have provided assessments on 13 countries seeking visa waiver status.

Also in March of this year, we came to an agreement with Germany on a terrorist watch list, fingerprint, and DNA exchange. This is becoming a model text for Visa Waiver Program members. We have taken a similar approach around the world on issues ranging from combating the use of fraudulent travel documents to taking down human smuggling and trafficking organizations.

Another initiative is the Security and Prosperity Partnership of North America, known as SPP, a core multilateral program that strengthens international intelligence collaboration. SPP was launched in March 2005 to increase security and enhance prosperity among the United States, Canada and Mexico through greater cooperation and information sharing. It includes key security and prosperity programs that cross mutual borders to keep them closed to dangerous people and subsequently open to trade. As part of the SPP, the United States has agreed to enhance intelligence partnerships with Canada and Mexico. For example, the United States and Mexico will form joint intelligence-sharing task forces along the U.S.-Mexico border to target criminal organizations and reduce violence along the border.

I know you heard earlier this week about the Mérida Initiative that is instituting a new paradigm for regional security cooperation among the United States, Mexico, and the countries of Central America, the Dominican Republic, and Haiti. This multi-year initiative is designed to build on activities already underway in the region and to complement U.S. efforts here at home, in order to reduce demand and trafficking of narcotics as well as arms and weapons, and to confront gangs and criminal organizations that cause serious security challenges for our international partners.

Our efforts to protect the nation from dangerous goods also entail international collaboration. In 2007, we launched our Secure Freight Initiative at six overseas ports. This was designed to test our ability to scan 100 percent of inbound cargo for radiation before the cargo was loaded on a ship bound for the United States. As a part of Secure Freight, we require that we obtain more information about what is in cargo shipments, and collect more trade data from the private sector. This gives us better visibility into the supply chain, and a more definitive ability to identify those kinds of shipments that require closer inspection. This is intelligence-based screening that helps us assure the security of our borders.

Complementing Secure Freight overseas, we also expanded our Container Security Initiative to 58 foreign ports. Using tools for scanning along with intelligence-derived information, DHS inspectors work with their foreign counterparts to screen cargo before loaded on to the ship. With the current deployment, more than 85 percent of the containers shipped to the U.S. now transit through these ports and benefit from our overseas inspections.

This level of cooperation with our foreign partners, occurring daily, has helped the United States apprehend dangerous people and keep dangerous goods from our shores. Although I cannot today share with you all the ways we are collaborating with our foreign partners, I believe these examples demonstrate how we are continually innovating our collaborative efforts with foreign partners to make sure dangerous people and goods are kept from entering our borders.

We recognize that, regardless of our differences, the United States and our international partners share common

security challenges and similar adversaries. The attacks on Madrid and London, and attempts in Germany and the UK over the past few years, underscore that reality. I am convinced that DHS will continue to strengthen our partnerships with our allies around the globe to expand our mutual ability to prevent any threat from jeopardizing our security interests.

Collaboration at Home

As I noted at the beginning, collaboration is needed at home as well as abroad. The best intelligence is meaningless if we do not have mechanisms in place to share it in a timely fashion with our operational partners. Central to our intelligence responsibilities is the sharing of intelligence and information with our State and local partners. As all of you know, prior to September 11, the U.S. Intelligence Community did not have a culture or common process of sharing across the Federal agencies, let alone with our State, local, tribal and private sector partners. I am proud to say today that building and improving our relationships with State, local, tribal, and private sector partners is the cornerstone of the Department's information sharing efforts.

As most of you are aware, the need to share information among Federal agencies—and for information and intelligence to flow from the Federal to State and local governments—was codified post-9/11 in several pieces of landmark legislation, such as the 9/11 Act. More recently, the President's amendments to Executive Order 12333 outlined new authorities for my Office, such as overt collection, and formally recognized "homeland security" as part of the national Intelligence Community. The new executive order specifically mandates greater information sharing with State, local, tribal, and private sector entities, which are core statutory customers and program partners of DHS Intelligence. Our DHS-unique collaboration challenge is to bridge the information sharing gaps between classified and unclassified, Federal and non-Federal, law-enforcement and non-law enforcement, as well as government and private sector domains.

I am pleased to say that over the past three years, we have developed strong relationships and collaborate closely with State and local law enforcement, first responders, and fusion centers nationwide to ensure State and local officials have access to key intelligence capabilities. Our outreach also helps to provide the Department an integrated intelligence picture using more tactical State and local information. Let me now highlight significant DHS actions to enhance collaboration with these key customers.

State and Local Program Office

As the 9/11 Act and the President's *National Strategy for Information Sharing* make clear, fusion centers are an essential part of this information flow and framework. These fusion centers have become the central points of exchange and centers of gravity for intelligence and information between Federal Government and State, local, and tribal entities. As you heard from Gary Winuk yesterday, fusion centers are developing a critical role in securing the homeland.

In 2006, we stood up a State and Local Fusion Center Program Office dedicated to supporting State and Local Fusion Centers throughout the country. DHS is committed to providing fusion centers with the people and tools they need to participate in the Federal Information Sharing Environment. As a key part of this effort, my Office is deploying intelligence officers to fusion centers nationwide. These officers are my representatives in the field who ensure that DHS is fulfilling its information-sharing responsibilities. Core activities of our intelligence officers include: providing daily analytic support; communicating and exchanging information with other fusion centers; writing products for and with State and local partners; and disseminating intelligence products to all customers. My Office will have officers in 35 fusion centers by the end of the year. We plan to eventually deploy up to 70 intelligence officers to the field, including one to each State-designated fusion center as well as major cities.

The presence of these important DHS personnel assets in the field has served to create strong collaborative relationships with our State and local partners. They serve as the front line of the DHS Intelligence Enterprise and help ensure that DHS is meeting these important customer's needs.

Access to Information Networks

DHS also provides our non-Federal partners with direct access to DHS intelligence and information through both classified and unclassified networks. A critical part of our efforts on the unclassified level is the Homeland Security Information Network's "Intelligence" Portal. Known as HSIN-Intelligence, this portal provides approximately 8,000 people with access to unclassified intelligence products. For classified networks, we are deploying the Homeland Secure Data Network, or HSDN, at fusion centers across the country. With this network, we are delivering, for the first time, classified threat information to State and local authorities on a regular basis. I believe this unprecedented type of communication will lead to a sea change in relations between Federal and State analysts.

To further expand State and local connectivity to the Intelligence Community, HSDN provides access to NCTC Online—for accessing the most current terrorism-related information at the Secret level.

We have also established the Homeland Security State and Local Intelligence Community of Interest as a means to develop and share information collaboratively. Known as HS SLIC, it is the first nationwide network of Federal, State, and local intelligence analysts focused on homeland security ever created in the United States. This virtual community of intelligence analysts fosters collaboration and sharing via weekly For Official Use Only-level threat teleconferences and biweekly Secret-level secure video teleconferences. As evidence of its value and success, its membership has grown dramatically from a six-state pilot in 2006 to now having members representing 45 states, the District of Columbia, and 7 Federal agencies. In addition, I have established an HS SLIC Advisory Board that includes State and local partners to advise me on issues relating to intelligence collaboration with our non-Federal partners. This gives me a chance to talk directly to key State and local leaders and hear how we can best collaborate with them.

Interagency Threat Assessment and Coordination Group (ITACG)

DHS also remains a full partner in, a leader within, and a staunch supporter of the Interagency Threat Assessment and Coordination Group, or ITACG. This group has become a vital mechanism for serving the information needs of our State, local, tribal, and private sector partners. Established at the direction of the President in his Guideline 2 report and the 9/11 Act, it pulls together Federal and non-Federal homeland security, law enforcement, and intelligence officers from a variety of disciplines to guide the development and dissemination of Federal terrorism-related intelligence products through DHS and the FBI to our non-Federal partners. ITACG officers monitor sensitive databases, and screen hundreds of highly classified finished intelligence reports to determine what should be sanitized and/or enhanced for expanded sharing with our non-Federal partners.

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 sets policy and oversees the ITACG Detail and its work.

The Detail achieved initial operating capability just nine months ago. 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. Currently there are three law enforcement officers from State and local police departments as part of the team assigned to the Detail. These non-Federal participants 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 10 in order to include a broader range of State and local expertise. Indeed, I would be remiss if I did not encourage all of you here from State, local, and tribal organizations to consider applying or encouraging one of your top performers to apply to serve on a one year detail at the ITACG.

We have also established the ITACG Advisory Council, which 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 with participation of its non-Federal members in all of its decision-making processes. I am extremely proud of the team we have assembled – both for the Detail and the Advisory Council. I am grateful for the strong support that I receive from NCTC in the overall management of the ITACG program.

Finally, we have trained reports officers in DHS components who gather local information of intelligence value. These reports officers provide this intelligence in the form of Homeland Intelligence Reports, known as HIRs, to the rest of the IC. Currently, we have over 30 reports officers located across I&A headquarters, DHS components and elements. In addition, four Reports Officers are deployed to State and local elements along the Southwest border and in Florida, with three more scheduled for deployment in the next few months. DHS reports officers have issued more than 9,000 HIRs since 2005 and in the process share valuable information on suspected terrorist activity, transnational threats from the Caribbean and Latin America, sensitive information from ports of entry including data from people who are given secondary screening, or people who are denied entry into the United States. This is precisely the granular-level of information that is of most use to the IC and State and local law enforcement authorities.

Challenges Ahead

Despite pride in the progress we have made in developing DHS Intelligence, we still have many challenges. First and foremost is the development of a high quality all-source cadre of analysts—this is extraordinarily difficult. Another great challenge is understanding the information needs of our many partners so we can ensure that the

right information—tailored as necessary—gets where it needs to be, when it is needed. Conversely, we need to help educate our partners on the kinds of information we need for our mission so we can access that information when needed.

We also have to work to find ways to work across different systems, processes, and legal systems to ensure a seamless flow of information. Not only do our international parties have different legal systems, but each of our State and local partners is also governed by different laws that can affect the flow of information. We have to find ways to bridge these differences.

We need to ensure that these efforts have sufficient funding, particularly for the fusion centers so they can continue to participate fully in these partnerships. Fusion centers cost money and many State budgets, particularly these days, simply cannot accommodate continuing robust efforts. Finally, throughout all these efforts we must be vigilant to protect civil rights, civil liberties, and privacy in all our intelligence activities.

Conclusion

On September 11 of this year, Secretary Chertoff wrote "...[on September 11, 2001,] our country was senselessly attacked and nearly 3,000 lives were tragically lost. That fateful day changed our Nation and our lives." Even though that day was more than seven years ago, the threat has not passed and the Nation's adversaries remain committed to harming us. They have been foiled by many factors, including the dedicated men and women of the Department of Homeland Security and our Federal, State, local, and private sector partners—many of whom are in this very room and defend our homeland every day.

Henry Ford once said: "Coming together is a beginning. Keeping together is progress. Working together is success." I am glad to report today that we are truly past the coming together and keeping together stages. We are now working together to keep this country safe. So we are achieving success. To prove this point, I just need to highlight the strong working relationship between DHS Intelligence and its national community partners, especially Director of National Intelligence Mike McConnell, FBI Director Bob Mueller, NCTC Director Mike Leiter, and the Under Secretary of Defense Intelligence Jim Clapper. These sound relationships form a vital backbone of Intelligence Community collaboration necessary to keep our country safe. I also can point to our many Federal, State, local, tribal, and private sector partners who work around the clock to protect our country and keep the American people safe, and who work with DHS every day. And last but not least our many international partners who help us stop threats beyond our borders.

Although a new team will be soon in charge in Homeland Security, the mission will not change and the need for collaboration will not lessen. I believe we are building the necessary relationships to continue to protect our nation from the myriad of threats that it faces. It is my steadfast belief that our level of collaboration shows we are up to the task.

Thank you.

This page was last reviewed/modified on October 30, 2008.