Remarks by Under Secretary Charles Allen at the Maritime Security Council

Release Date: October 7, 2008

Washington, D.C.
Maritime Security Council 2008 Leadership Summit
(Remarks as Prepared)

Introduction

Mr. Murray, distinguished guests, ladies and gentlemen. It is a pleasure to speak to you this morning on the maritime threat to the global supply chain. Maritime security is a topic important not only to the Department of Homeland Security, but to everyone in this room, and indeed in this country. Our purpose today is to find ways to work together to improve our ability to warn of threats to the United States. Our common purpose is to keep the nation safe. Thomas Jefferson recognized this great calling when he noted that for all Americans "eternal vigilance is the price of liberty." Today we follow in his footsteps confronting the 21st century threats to our security – threats that I view as very serious. The world in certain ways has grown darker.

As an individual who has labored long in the crosscurrents and eddies of the muddy waters of intelligence and spent a considerable portion of that time working warning issues, I am acutely aware of both the importance and the challenges for threat warning and threat assessment. My own experience with the topic of maritime security began with the 1985 hijacking of the Achille Lauro by four members of the Palestinian Liberation Front. At that time, our focus was on the impact that event had on Israeli-Palestinian relations. We failed to perceive this act as the precursor of what has become a significant threat to our maritime-based supply chain. And we must remember that the terrorists who were captured at Sigonella, Italy, did not originally intend to hijack the Achille Lauro.

Importance of the Maritime security

You know better than I the importance of the maritime component of our global supply chain. The National Strategy for Maritime Security captures this best:

"In today's economy, the oceans have increased importance, allowing all countries to participate in the global marketplace. More than 80 percent of the world's trade travels by water and forges a global maritime link. About half the world's trade by value and 90 percent of the general cargo, are transported in containers. Shipping is the heart of the global economy . . ."

According to a United Nations assessment, container traffic will grow from 192 million TEU (twenty foot equivalent units) in 2005 to 492 millionTEU in 2015. This is an average increase of 9.5 percent per year. Container shipments into U.S. ports are massive. In 2006, more than 31 million containers entered ports in New York and New Jersey, and almost 14 million arrived in Savannah and Seattle. Even in my home state of North Carolina, nearly a million containers entered the port of Wilmington. This activity is clearly the engine that drives not only our economy, but the global economy as well. Disruption of this complex, sophisticated, efficient system would wreak havoc on our nation and deeply affect the global economy. To borrow from a recent book by Steve Flynn, we are on *The Edge of Disaster*.

Two of the scenarios that Flynn presents are worth mentioning briefly to highlight the significance of supply chain disruptions. He describes potential terrorist attacks on shipping; the first involves liquid natural gas (LNG) deliveries to Boston Harbor and the second is sinking a large ship to block the channel to the port of Los Angeles. Both of these scenarios draw attention to the impact to the supply chain that terrorist attacks could potentially achieve. In each case, it is not just the immediate impact on the loss of LNG in New England, or the blockage of the shipping channel in Los Angeles. It is the broader impact of the loss of electric power and other secondary effects in Boston, and the impact of gasoline supplies on the auto dependent economy of southern California that truly demonstrate the impact of such attacks on the entire supply chain. Economic losses from these events could result in billions of dollars per day. Given the complex nature of just-in-time deliveries from

global suppliers and low inventories to reduce costs, the potential economic disruptions could be massive.

Threats to the Maritime Supply Chain

WMD

My primary concern is the threats that could affect maritime security and have an impact on the homeland. Of most concern, in terms of consequence, is the introduction of a weapon of mass destruction into the homeland through our ports and harbors. While we currently assess that al Qa'ida lacks a WMD capability, it is equally clear that they intend to obtain this capability and would not hesitate to employ such a device should they obtain one. Since terrorists lack a missile delivery capability for such weapons, our concern is their use of the supply chain to deliver a device directly and employ it in a major city. Such an attack has been justified by radical cleric Shayk al-Fahd in the following chilling terms: ". . .if those engaged in jihad establish that the evil of the infidels can be repelled only by attacking them at night with weapons of mass destruction, they may be used even if they annihilate the infidels."

As you are well aware, the Department and its components have implemented a number of initiatives to better secure the supply chain, including DHS, CBP and ICE inspectors working with their counterparts in foreign ports to screen containers and to identify high-risk shipments, which are then subjected to nonintrusive inspection using large scale X-rays and radiation detectors. Our partnership with those of you in the private sector is critical to the success of these efforts, which have been most comprehensively addressed in the Strategy to Enhance Global Supply Chain Security (July 2007). These efforts seek to balance carefully the needs of security with the need to maintain global commerce and increased confidence in both the safety and timely arrival of goods and people.

Terrorists

It is not just the potential for WMD that is a threat to the maritime security, however. As I mentioned earlier, my focus on this problem began in 1985 with the Achille Lauro hijacking. Since then, a variety of terrorism events have demonstrated the potential for seaborne attacks to impact various aspects of the maritime supply chain. In the late 1980s and into the 1990s, there were a series of ferry hijackings designed to highlight terrorist causes or to undermine the tourist economy. These included the Chechen seizure of a Turkish ferry on the Black Sea and al-Gama al Islamiyaa targeting of Nile River passenger boats. In 2004, the Abu Sayaf Group bombed the Philippine "Superferry 14," killing 116 -- the most deadly attack to date.

Terrorists have also used maritime attacks to achieve economic effects. The 2002 bombing by a small boat with 220-440 lbs of TNT of the M/V Limberg off the coast of Mulkalla, Yemen resulted in one crewman killed and 50,000 tons of oil being spilled in surrounding waters. In April 2004, suicide attacks by al Qa'ida operatives closed two offshore oil terminals for two days and cost $40 million in repairs.

Fortunately, all these attacks occurred far from our shores and were not catastrophic. But they provide examples of what terrorist organizations can achieve with very modest capabilities. Over the 20 plus years that I have been working on terrorism issues, these types of attacks have spread from the eastern Mediterranean to the Arabian Gulf and Red Sea to the Philippine Sea. I remember painfully the attack on the *USS Cole* on 12 October 2000. This raises my concern regarding the possibility that one day, maritime attacks will reach our shores. And not just by foreign-based operatives. Of increasing concern to me and the Department are homegrown extremists.

Homegrown Extremists

To date, we have been very fortunate that the homegrown extremists we have apprehended, the Fort Dix conspirators and the John F. Kennedy airport plotters, have lacked expertise and demonstrated poor operational security. Consequently they were identified and arrested before they could launch their attacks. We are not likely to benefit from this carelessness forever.

In this regard, I highlight the importance of the Transportation Worker Identification Credential and REAL ID programs in providing secure identification for those with access to our ports facilities, whether that access is via ship, rail, or road. Being able to separate those with legitimate business from those who do not is a key step in providing useful suspicious incident reporting that could reflect preattack surveillance, planning, or rehearsals.

For example, following the bombing of the USS Cole, we in the intelligence community and the FBI reconstructed

the planning and preparation by Abdul al-Rahim al-Nashiri, the al Qa'ida mastermind of the attacks. Two factors stand out for our discussion today:

1. Target surveillance gleaned the critical information that the refueling window for U.S. warships was four hours, the time available to conduct the attack.
2. A rehearsal vastly improves the chances of success. On their first attempt on the USS The Sullivans, the attack vessel was overloaded with explosives and sank after leaving the dock.

The types of activities that could reflect preattack surveillance, planning, or actual rehearsals are the essentials of warning intelligence. It is my hope that in your deliberations later today you develop an understanding of the importance of this information and the reliance that we place on our state, local, and private sector partners to provide support in this important area.

Drugs, Alien Smugglers, and Criminals

While my remarks have thus far focused on foreign and homegrown Islamic terrorists, I would be remiss in not identifying other potential actors that may have impacts on maritime security. These include drug and alien smugglers who subvert vulnerabilities in the supply chain to move drugs and humans illegally. They are a scourge on our society and the efforts we have under way to secure the supply chain will limit their ability to exploit the system illegally.

Since the founding of our Republic, smugglers have used legitimate shipping activity to import contraband. Today, technically savvy and highly organized transnational criminal groups have replaced the vagabond pirates of Jefferson's time and reflect the globalization of our world. Their activities support or engage in drugs, alien smuggling, and contraband such as illegal arms. They also include financial crimes and money laundering, which brings me to the final threat issue I want to raise with you.

Cyber Threats

Just as criminals have moved into the cyber world to conduct financial criminal activity, the threat of cyber attack is an emerging threat to the maritime security. As the DHS Strategy to Enhance Global Supply Chain Security notes, the supply chain is not just goods, it is also information about those goods. As you know better than I, ships and port facilities are highly automated. The range of actors who could develop the skills to hack into these systems is growing. Not only foreign terrorist groups, but also domestic extremists like the Animal Liberation Front or various anarchist groups that reject globalization, are potential sources for extremists with hacking skills to focus their efforts on the automated systems supporting maritime commerce. This is also a key area in which a disgruntled insider could use high-tech skills and access to impact the flow of goods through misrouting. These actions could have significant real impacts not just on the movement of material but also on production centers dependent on the timely arrival of this material to use for assembly or for final sale.

Role of DHS Intelligence

The common thread that ties together DHS' efforts to address this maritime security issues is effective information collection, analysis, and sharing. Reliable, real-time information and intelligence allows us to identify and characterize threats, target our security measures, and achieve unity of effort in our response. Secretary Chertoff said it best on 14 July 2005 when he stated that "intelligence is at the heart of everything DHS does."

Intelligence is not only about spies and satellites. It is about the thousands and thousands of routine, everyday observations and activities. Surveillance, interactions – each of which in isolation is not a particularly meaningful piece of information – but when fused together, gives us a sense of the patterns and flows that are the core of what intelligence analysis is all about.

Lest we lose sight of the threats to our country from dangerous people and dangerous goods, think of the enforcement activities the Department carries out every day:

- Customs and Border Protection 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. We harvest the intelligence information they possess.

- Immigration and Customs Enforcement seizes more than $700,000, makes 150 administrative arrests and 61 criminal arrests, removes some 760 aliens and participates in an average of 20 drug seizures.
- The Transportation Security Administration 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 $12.9 million.
- The U.S. Secret Service seizes an average of more than $145,000 in counterfeit currency and more than $50,000 in illegal profits, and conducts nearly 20 arrests.

These encounters generate a treasure trove of data that we are just now learning how to report, collate, and share. This means that DHS is a collector, producer, and consumer of intelligence, which makes my work that much more challenging.

Information Sharing

To understand these threats sharing of information is vital. Let me briefly sketch out my vision and what we have accomplished with our state and local partners. Each level of government has unique and valid missions and responsibilities regarding Homeland Security Intelligence. We work at varying levels of classification and have different sources. Analysts have different skill sets and priorities. At times it seems that surmounting these challenges to create an information environment that flows from the federal to the state and local officials and from state and local officials back to the federal level seems almost impossible to achieve. But if we can sustain our vision and overcome the obstacles, the qualitative and quantitative benefits of improved information sharing across our organizations can become an extraordinarily valuable tool in our efforts to provide homeland security.

If I may I'd like to read to you what the President said at the DHS 5th anniversary event in Washington last March:

"The Department of Homeland Security is working to strengthen cooperation with state and local governments -- so we can prevent terrorist attacks, and respond effectively if we have to. Before 9/11, the federal government sent threat information to authorities -- local authorities by fax machine. Today, we've established 21st century lines of communication that allow us to share classified threat information rapidly and securely. We've helped state and local officials establish intelligence fusion centers in 46 states. These centers allow federal officials to provide intelligence to our state and local partners, and allow locally generated information to get to officials here in Washington who need it."

To expand on our current capabilities, I envision a network of state, local and federal intelligence and law enforcement professionals working together – supported by appropriate tools – to achieve a common goal: protection of the nation.

Working together – leveraging Federal as well as State and Local networks; moving relevant information and intelligence quickly; enabling rapid analytic and operational judgments – that is what this National Fusion Center Network is all about.

Our ability to move, analyze and act on information is our greatest strength. We must use the network and the information in that network, to push our defensive perimeter outward.

That's what the National Fusion Center Network will do for us.

Intelligence officers armed with the appropriate tools help to push the edges of the National Intelligence Community out to the states, and bring the power of that community to bear on the problems of the states. In addition, information once only available in cities and states can be used to protect the nation as a whole.

This is all very new and different for the Intelligence Community. We are working hard to educate ourselves to your information needs, as well as increase our ability to provide you information.

And we all must do this while paying the utmost respectto the civil liberties and privacy of our citizens.

Let me speak to what we have accomplished;

- We now have 25 officers deployed to fusion centers with a goal of 10 more by the end of the year. We have expanded the SECRET-level Homeland Security Data Network to 23 sites and will double that number by the end of the year. From a staffing and IT perspective, we have made significant gains.

- Equally important, this improved connectivity is resulting in expanding intelligence production. So far this year nine intelligence assessments have been produced with the fusion centers, DHS and other partners. One of particular note, four fusion centers collaborated on a product -- *The Barcelona Terror Plot*(by Los Angeles JRIC, Sacramento RTTAC, Maryland MCAC, and Ohio SAIC) -- based on the support and experience they had with DHS.
- This is not a one way street with information and products flowing to the state and local customers. DHS' Office and Analysis has initiated the delivery of unique state- and local-origin information for use by the national Intelligence Community. More than 140 Homeland Intelligence Reports have been written this year using this nontraditional source of information. Last year this reporting stream accounted for 1.5 percent of our reporting; so far this year it accounts for 8.0 percent of our reporting. In two cases, IC analysts used local information to write articles for the President's Daily Brief. Without the presence of a DHS officer in the state fusion center, this information would not have been available. This is the essence of the effort to share intelligence and information vertically and horizontally.
- In anther case, a state police agency provided encounter information garnered during a traffic stop to a fusion center. The fusion center, recognizing the value of the data, made it available to Immigration and Customs Enforcement. ICE reviewed the information, an I&A intelligence officer did some more research, and ICE was able to affect an arrest in another state.
- We built web pages for each fusion center on HSDN to enable information sharing. Now anyone with SIPRNET access can have access to products written in the states.
- We have added more users to the unclassified Homeland Security State and Local Community of Interest – the HS-SLIC. We now have 45 states, the District of Columbia and seven federal agencies collaborating in that network.
- In information sharing, we also are leading – under the management of the National Counterterrorism Center – the Interagency Threat Assessment and Coordination Group (ITACG), which ensures that "federally coordinated" information relating to threats are rapidly and effectively disseminated to the fusion centers.
- Working with our partners across the community, we are implementing a Suspicious Activities Report system to capture valuable information from the eyes and ears on the ground maintained by local law enforcement.
- We have developed a plan to provide mobile intelligence training teams on site at the fusion centers. We will kick off this training next month. The Offices of Privacy and Civil Right and Civil Liberties have developed a deployable training module as well.

Now let me address some of the continuing challenges:

- For all of us at any level of government, obtaining funding for our information-sharing needs remains an issue both in terms of equipment and in terms of personnel we can train to become experienced intelligence analysts.
- Second, training, processes and policies need to be strengthened at all levels to ensure that we extract maximum advantage from our information-sharing program
- Third, recognizing the reality of different priorities and different levels of expertise and analytical focus are required to understand how we can practically improve our information-sharing efforts.

Finally, I would add a slightly different challenge. The need to experiment; to see what works.

Importance of our Private Sector Partners

It is not just data that DHS and its components collect, process and disseminate that is important. The Director of National Intelligence (ODNI) initiative led by Rear Adm. Kelly through the Global Maritime and Air Intelligence Integration effort represents a critical component in our cooperative efforts to gain the Marine Domain Awareness that supports improved maritime security.

In January 2008, the USCG Intelligence Coordination Center, in coordination with the Domestic Port Security Evaluation and my Critical Infrastructure Threat Assessment Division, became the first agencies to apply the USCG Maritime Security Risk Analysis Model (MSRAM) approach to a strategic, maritime terrorism threat assessment for the Homeland. The National Maritime Terrorism Threat Assessment —-an unclassified product suitable for homeland security enterprise use—-was a pragmatic application of risk intelligence to support operational planning and national policy decisions involving port security grants and related legislation.

The primary dissemination venues for the National Maritime Terrorism Threat Assessment and other "sensitive but unclassified" threat information products to members of the Maritime Security Committees include the MSRAM Program Coordinator for each USCG Sector and several sensitive but unclassified Internet-enabled Web site portals, such as HOMEPORT, Law Enforcement Online (LEO), INTELINK SBU/Intellipedia, and the Homeland Security Information Network (HSIN). Since January 2008, DHS subcomponents have disseminated more than two dozen HOMEPORT, LEO, and HSIN threat-related products disseminated nationally to Maritime Security Committees. Moreover, each of these documents has been posted to Intellipedia -- an ODNI INTELINK-based collaborative environment where analysts, law enforcement, governmental, private sector, and academic experts in diverse locations can work together in a near-simultaneous fashion on common threat assessment projects. In concert with the USCG and other federal agencies, the Office of Naval Intelligence (ONI) interacts with industry via the International Council of Cruise Lines (ICCL) Security Director's quarterly meeting. ONI also produces the Worldwide Threat to Shipping Message (WWTTS) that is disseminated via NGA NOTAMS and the World Wide Web. The former meeting identifies threats to cruise lines globally, while the latter message highlights global threats to mariners from maritime crime and piracy.

But a lot depends on you. As owners and operators of our maritime resources, you are closest to the action and will have the first indications and insights that can provide us both potential warning and an ability to respond to prevent an attack. I appreciate your support and efforts to help us cooperatively develop improved processes to generate more effective information sharing and threat warning in the maritime domain.

Conclusion

In closing, I am reminded of the words of Edmund Burke: "All that is necessary for the triumph of evil is that good men do nothing." I commend you for "doing something about it " both in your attention today and in the work you do everyday. Defeating the threats I have described is critical to protect the global maritime supply chain, which is the lifeblood of our economy and critical to the security of our homeland. It is only with your help that we can improve our ability to provide the warning essential to achieve this task. Thank you for your time and attention.

This page was last reviewed/modified on October 7, 2008.