THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 5 NUMBER 3

SEPTEMBER 2006

9/11: FIVE YEARS ON

Contact: CIPP01@gmu.edu
703.993.4840

Click here to subscribe. Visit us online for this and other issues at http://cipp.gmu.edu

In commemorating the five year anniversary of September 11, 2001, as well as recognizing National Preparedness Month, we sought the voices and reflections of leaders throughout government and industry. We are very pleased to be able to share a contribution by George Foresman, Under Secretary for Preparedness, and in addition to his reflections, we also present the DHS Fact Sheet "Protecting the Homeland Post September 11" in its entirety, as it clearly captures the work done during the past five years.

To further enrich and round-out this issue, we sought and received numerous contributions from the private sector reflecting on the progress made since 9/11. In addition to these voices, we also had the opportunity to interview Phil Lacombe, Former Director of the President's Commission on Critical Infrastructure Protection (PCCIP), on his views on cyber security progress since 9/11.

We also capture components of the testimonies of Steve Simon and Richard Falkenrath at the Senate Homeland Security and Governmental Affairs Committee on "Homeland Security: The Next Five Years" held on September 12, 2006. These statements, as well as an op-ed piece by former Governor of Virginia Mark Warner, provide further insight into the immense work and effort undertaken by all levels of government in the past five years. Our Legal Insights column recounts a portion of the major terrorism cases by individuals and groups arrested and prosecuted for planning attacks against the United States. We have also included reader commentary to last month's Legal Insights.

September has been a busy month for the CIP Program, having hosted a 9/11 commemorative event with Governor Warner on September 5, released our new book, *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*, and preparing for another Critical Conversation event for National Preparedness Month on September 27, 2006 at the National Press Club.

Finally, it is with sadness that I note the passing of Admiral Bill Kime, U.S. Coast Guard (ret). Admiral Kime was the 19th Commandant, and as a young Lieutenant Commander, I was privileged to serve as his personal Aide. A visionary leader, Admiral Kime was a pioneer of critical infrastructure and homeland security. Among his many accomplishments, he will be remembered for his extraordinary and tireless work with the maritime industry. His wisdom, technical knowledge and high ethical standards were respected by all, and always fostered a frank and forward-moving discussion between the public and private sector – setting today's standard. Additionally, in the aftermath of the Exxon-Valdez disaster, Admiral Kime led the reengineering of the national response process and helped set the nation on a better footing to deal with incidents of national significance. The Admiral was a gifted officer, visionary public servant, and wise mentor to many. He will be sorely missed.

As always, thank you for your continued support of the CIP Program.

John A. McCarthy
Director, CIP Program
George Mason University, School of Law

Understanding Preparedness

George W. Foresman, Under Secretary for Preparedness
U.S. Department of Homeland Security

While much focus has recently been placed on hurricanes in light of Katrina and in the context of the current hurricane season, the Department of Homeland Security is focused on a broad national preparedness agenda with an all-hazards risk management approach. The way we respond to emergencies should not reflect the type of hazard; it should reflect a risk continuum. Preparedness is about establishing an integrated method of actions that focus and unify how, as a nation, we coherently manage, respond, recover, prevent, and protect across the full spectrum of risk.

Part of this effort is understanding that national preparedness reflects an approach where the three levels of government, the public and private sectors, and the American people operate with unified purpose to manage risk from individual, community and governmental perspectives. Under a national approach, parallel actions at the federal level complement state and local activities. Strengthening America's preparedness requires sustained commitment among Congress, federal agencies, local and state governments, the private sector, and the American people. September is National Preparedness Month, which highlights the importance of preparing citizens for a broad range of possible threats. A prepared citizenry is key to our national preparedness success. National Preparedness Month is a nationwide coordinated effort held each September to encourage Americans to take simple steps to prepare for emergencies in their homes, businesses and schools. The U.S. Department of Homeland Security is sponsoring National Preparedness Month 2006, centered on family emergency preparedness. The Department is working with a wide variety of organizations, including more than 650 national, regional, state and local organizations that form the National Preparedness Month Coalition, highlighting the importance of public emergency preparedness throughout September and beyond. The National Preparedness Month Coalition members will distribute emergency preparedness messages to their customers, members, employees, stakeholders and communities across the nation.

> "Preparedness is about establishing an integrated method of actions that focus and unify how as a nation we coherently manage, respond, recover, prevent, and protect across the full spectrum of risk."

The goal of National Preparedness Month is to increase public awareness about the importance of preparing for emergencies including natural and man-made emergencies and to encourage individuals to take action to prepare themselves and their families. The month provides Americans with a variety of opportunities to learn more about emergency preparedness. Events and activities across the nation will encourage individuals to get an emergency supply kit, make a family emergency plan, be informed about different threats, and get involved in preparing their communities.

As an example of the type of activities that are part of National Preparedness Month, the Department recently announced a partnership with the American Association of Retired Persons, the American Red Cross, the National Organization on Disability, and the National Fire Protection Association. This joint effort allows us to broaden our message to older and disabled Americans, two of many particularly vulnerable populations that may bear the worst effects of any disaster.

It also is a chance to reinforce to the American public that the responsibilities for our safety and security transcend government, the private and non-profit sectors. Americans have a critical role for their own safety and security. Accordingly,
(Continued on Page 27)

Private Sector Perspectives on the Journey Since 9/11

The Electric Sector

Stan Johnson
North American Electric Reliability Council
Manager, Situation Awareness and Infrastructure Security
ESISAC Team Member

As our nation sorts through the full range of thoughts and emotions generated by the fifth anniversary of 9/11, the electric sector also pauses to reflect on how sector concerns have shifted since 9/11, the progress we have made in addressing those concerns, and the challenges that lie ahead as we work to secure our nation's critical infrastructure.

Having navigated through the Y2K event prior to 9/11, the energy sector felt fairly confident about the security and reliability of its portion of the nation's critical infrastructure. Nevertheless, the sector was dealing with the continuing challenge of deregulation and the problems experienced in California in 2000. Additionally, several large mergers had recently been announced in the industry, and the rapid pace of change promised to continue for many years.

Since 9/11, the sector has adapted to the nation's changing needs. While the August 14, 2003 Northeast Blackout was a wake up call for the sector, industry members have responded by effectively implementing several initiatives. For example, critical infrastructure protection (CIP) initiatives have advanced rapidly in the sector. The Electric Sector Information Sharing and Analysis Center (ESISAC) began operation in 2003. The Critical Infrastructure Protection Advisory Group (CIPAG) began meeting with a wide-range of representatives from across the sector. The CIPAG has evolved into the Critical Infrastructure Protection Committee (CIPC) with 36 members, who are industry experts in the areas of cyber security, physical security, and operational security from the U.S. and Canada. The executive committees of CIPC, along with the CEO of the North American Electric Reliability Council (NERC), were designated as the Electric Sector Coordinating Council (ESCC) and now meet regularly with its government partners from the Department of Homeland Security, the Department of Energy, and the Federal Energy Regulatory Commission. Seventeen security guidelines were approved by CIPC and have been adopted by the NERC Board of Trustees for use across the energy sector. In addition, the Energy Policy Act of 2005 was signed by President Bush, and NERC has since been designated as the Electric Reliability Organization (ERO).

Though our progress has been strong since 9/11, much remains to be accomplished. Our focus over the next five years will be in these six areas:

Implementation of new cyber security standards: The recently passed cyber security standards, CIP 002-009, will require considerable attention and resources to secure the sector's cyber assets.

Transition of NERC to the ERO: NERC's transition to the ERO and the sector's full enforcement of mandatory reliability standards will be a rewarding challenge for the industry.

Formation and modernization of new security guidelines: The development of new security guidelines and the updating of existing guidelines will keep the sector current with the latest innovations in CIP and technology.

(Continued on Page 25)

The Real Estate Sector

Roger Platt
Senior VP and Counsel, The Real Estate Roundtable
Executive Director, The Real Estate ISAC
Co-Chair, Commercial Facility Sector Coordinating Council

The real estate industry is among the critical infrastructure and key resources impacted by the recent terrorist threats facing the United States. As airplanes struck the two largest office complexes in the United States on 9/11, they also eviscerated a large and thriving 22 story hotel in World Trade Center III and a huge shopping mall (more than 427,000 square feet of retail space) in the World Trade Center's concourse mall. Two years later, our government discovered Al Qaeda plans involving apartment buildings in New York City. Operatives were planning to rent the units, seal them with duct tape, fill them with gas from their own utility-fed gas lines, and detonate them externally.

Before 2001, the perceived risk of terror attacks on large commercial real estate facilities was so low that insurance companies routinely covered it as part of typical "all risks" policies. That practice changed dramatically after the attacks on the World Trade Center and the Pentagon, and the issue became a high priority for any landmark real estate. Indeed, in the weeks and months following the attacks of September 11, our sector concluded that the complex and evolving nature of this terrorist threat demanded strong leadership from government and our sector — and close coordination between the two — to ensure that we were working together to manage risk in the interest of all Americans. As stated by a prominent real estate executive in testimony before a Congressional subcommittee:

"We are always looking for ways to better manage the risk of further threats and attacks. At the same time, we remain very dependent on the ability of government (including mass transit authorities) to help limit the ability of terrorists to reach our facilities in the first place . . . We know our buildings' individual vulnerabilities; government has more of a beat on the changing threat environment. We both need each other to succeed."

Since 9/11, the real estate industry – collectively through The Real Estate Roundtable (RER) and its various real estate trade association partners – has pursued a broad range of activities to help individual businesses better manage the extraordinary challenges of owning and operating property in these uncertain times. These activities include:

- Sharing threat-related information with the Department of Homeland Security (DHS) through the Real Estate Information Sharing and Analysis Center (ISAC) and the Commercial Facility Sector Coordinating Council (CFSCC);

- Developing and expanding partnerships with local law enforcement and emergency response officials at all levels of government;

- Identifying and facilitating opportunities to improve emergency preparedness throughout our industry and the broader commercial facility sector;

- Advocating for federal policies such as terrorism risk insurance legislation, risk-based security funding, and targeted tax incentives for security-related investments; and

- Supporting sophisticated, credible research on terrorism risk management through our partnership with the RAND Center for Terrorism Risk Management Policy.

While RER and its real estate trade association partners have worked to support the operations of individual businesses, many individual companies have also pursued their own infrastructure protection efforts. According to the Building Owners and Managers Association International, average security related spending at individual companies is

(Continued on Page 28)

The Chemical Sector

Chemical Sector Coordinating Council
Beth Turner, Chair (DuPont)
Rick Kane, Vice Chair (Rhodia)

The tragic events of September 11, 2001, forced many industries to alter the way they conduct business, and the chemical industry was no exception. While the sector had recognized the importance of security before that date, since 9/11 the chemical industry has incorporated security into every aspect of its business. The chemical industry had previously integrated safety throughout the chemical manufacturing, distribution, storage, and use life cycle, and this successful effort has served as a model for security enhancement. While great strides have been made over the past five years by many members of the chemical sector, we can still do more to fulfill our collective obligation to our workers, our shareholders, our communities, and the American people.

As part of our commitment to increase chemical industry security, chemical facility owners and operators have spent great sums of money -- $3 billion by members of just one trade association -- on facility security improvements such as improved perimeter barriers, tighter access controls, better surveillance, new process controls and equipment, enhanced information/computer security, and more stringent background checks. Several chemical industry associations now require their member companies to perform facility vulnerability assessments and implement protective measures to ensure that every member facility meets a baseline level of security. Some leading companies have created the Chemical Sector Cyber Security Program to drive improvements in cyber security within the sector and its IT providers.

In addition to those independent efforts, members of the chemical industry have worked closely with the Department of Homeland Security (DHS), the Federal agency responsible for coordinating chemical industry security efforts, since DHS was established in early 2003. Collaboratively, DHS and members of industry have established mechanisms to share chemical industry threat and security related information; refined consequence and vulnerability assessment methodologies for use by chemical facility owners and operators; jointly performed assessments of the security postures of some of the potentially highest-risk chemical facilities and the Federal, state, and local response capabilities of the communities in which those facilities are located; and piloted protective measures at selected facilities for potential use across the industry.

To help coordinate these individual and joint efforts, members of the chemical industry have created the Chemical Sector Coordinating Council (CSCC). The CSCC—comprising seventeen chemical industry associations whose membership is believed to make up a majority of the nation's chemical manufacturers, distributors, and warehousers—serves as a forum for the chemical industry to discuss and coordinate sector-wide security issues and a reliable and efficient way for DHS to communicate with it. A government counterpart, the Chemical Sector Government Coordinating Council (GCC), has been established and is being chaired by DHS to ensure coordination among the various Federal departments and agencies, like the FBI, who work with the chemical industry on security concerns. Under the auspices of the Critical Infrastructure Partnership Advisory Council, members of the SCC and GCC can consult and formulate recommendations regarding the best ways they can jointly protect the industry and enhance its security.

The events of 9/11 have changed the world and the way businesses must operate. Of its own accord, the chemical industry has mobilized and is actively working to address the new threats facing its members. Through these efforts, including close collaboration with DHS and other security partners, the chemical industry will meet this new challenge, and will continue to contribute to the well-being of individual Americans and the nation as a whole, safely and securely. ❖

The Dam Sector

Lyman Shaffer, Chair (Pacific Gas and Electric)
Dam Sector Coordinating Council

Historically, security concerns within the dam sector have been largely focused on minor criminal activities such as trespassing and vandalism incidents, including threats to the sector from environmental activists. Large private sector dams are typically owned and operated by electric generation companies, most of which have professional corporate security organizations that manage security matters within their overall portfolio of assets that include fossil power plants and large electric transmission and distribution structures. Large dams used for water storage and distribution are often owned by municipal or special district agencies. Relatively few small dam owner-operators, whether private or government owned, had organized security programs prior to 9/11.

Since 2001, the federally licensed dam owner-operators have worked collaboratively with the Federal Energy Regulatory Commission (FERC) Division of Dam Safety to develop security guidelines for federally licensed dams. These included a requirement that security assessments be conducted on dams designated to have higher security requirements, and those results are reviewed by FERC Regional Inspectors as part of their annual safety inspection programs. In addition, FERC and non-federal dam owner-operators formed a Dam Security Working Group which met periodically, particularly as part of Dam Security/Safety seminars conducted annually since 2003 and attended by a wide range of dam owners including federal, state, and municipal dam owners. That group was superseded by the establishment of the Dam Sector Coordinating Council (DSCC) and its Federal counterpart, the Government Coordinating Council (GCC).

The DSCC was formed in May 2005, and is currently composed of 23 members representing owner-operators throughout the United States and Canada. It also includes trade associations representing a broad range of owner-operators from across the sector. The council is currently recruiting additional representation from water sector dam owners. The DSCC has met quarterly since its formation and has been actively involved in the development of the current version of the Dam Sector Specific Plan (SSP), as well as regularly participating in the Partnership for Critical Infrastructure Security (PCIS) and the National Infrastructure Advisory Council (NIAC) activities. The council also closely coordinates with the Electricity SCC.

The DSCC works closely with the GCC under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC). As part of ongoing efforts, the DSCC and the GCC have formed a number of joint working groups to address the following dam security issues: cyber security, information sharing, security education, asset identification, R&D, and RAM-CAP development. The DSCC has also established ongoing liaison efforts with the Homeland Infrastructure Targeting and Analysis Center (HITRAC) and DHS's National Cyber Security Division (NCSD).

As established in the current version of the Dam SSP, the SCC is committed to expanding outreach throughout the dam sector, particularly to small dam owner-operators who do not have dedicated security staffs, over the next few years. One initiative is the development of the dam sector Homeland Security Information Network (HSIN) portal which provides a web-based vehicle for effective outreach across the sector particularly for alert and event notification as well as educational purposes. The SCC is compiling relevant generic security education materials to be used by small dam owner-operators to develop and implement security programs. The DSCC is considering using HSIN and the trade associations to make these materials more widely available. The DSCC is also supporting R&D efforts over the next several years to better define threats unique to the sector, as well as cost effective mitigation measures particularly related to protection of facilities

(Continued on Page 27)

The Financial Services Sector

George Hender, Chairman
Financial Services Sector Coordinating Council

On the morning of September 11, 2001, the major players in the financial services sector had robust disaster recovery and business continuity programs in place. Years of work on Y2K issues had contributed to the advanced state, relative to other sectors, of business continuity plans among financial services firms. By the end of the day, however, it was clear we needed to rethink our approach to business continuity planning (BCP).

Prior to 9/11, disaster recovery and business continuity focused on infrastructure rather than resources. Back-up sites existed, but generally as empty rooms without staff. The magnitude of the loss of life on 9/11 prompted a reevaluation that made people a central consideration in BCP. Almost immediately, a number of firms—particularly core clearing and settlement firms—dispersed staff among different locations. Over the past five years, the sector has spent hundreds of millions, if not billions, of dollars to build in redundancy and spread the workforce among different locations to avoid a single point of failure.

The most significant efforts of the financial services sector in the five years since 9/11 have come in the area of communication. The terrorist attacks served as a reminder of just how interdependent we are. Firms have, therefore, built new systems and procedures to communicate with employees, customers, vendors, utilities, and regulators during and following a crisis. To avert economic disruption on a wide scale, the financial services industry has developed better communication with federal agencies on security matters. The primary mechanism for this communication is the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). FSSCC works with its members and the government to assemble the best information available on handling crises from terror attacks and blackouts to hurricanes and pandemics. One of FSSCC's major roles in a crisis is to ensure an efficient two-way information flow between private and public sectors.

During the past five years, the financial services sector has also conducted a vigorous regime of testing its preparedness. Last year, a successful market-wide test across the securities, fixed income and derivatives industries provided the opportunity to submit, execute and settle test orders from back-up sites.

The attacks of 9/11 showed that business continuity planning could not be done in the isolation of a single firm. The challenge of the coming years is to broaden the planning across sectors. A recent report issued jointly by the Federal Reserve, Securities and Exchange Commission and the Office of the Comptroller of the Currency recognized the financial sector as one of the most resilient commercial sectors, but noted it "cannot fully protect against infrastructure disruptions of telecommunications, and it can only provide limited resilience against disruptions in other elements of critical infrastructure, such as power, transportation and water."

To address these cross-sector interdependencies, the financial services industry, through the FSSCC, is now working with representatives of the sectors upon which we depend for power, telecommunications, and basic operations to ensure our increased resilience is being matched.

The nation's banking, securities and insurance firms have been actively working to strengthen the financial infrastructure over the past five years, and will continue to work to ensure it can meet the financial needs of Americans in the event of a disaster—whether man-made or natural. ❖

CIP: Past, Present and Future

The CIP Report conducted an interview with Phil Lacombe, Former Director of the President's Commission on Critical Infrastructure Protection (PCCIP), and current Senior Vice President and General Manager of the Integrated Systems and Security Business Unit, SAIC.

America has yet to experience a massive Internet disruption in which service is unavailable for days, weeks or months. For the next terrorist attack on American soil most agree that it is not a question of "if" but "when." Does the same hold true for a massive attack on the Internet?

Lacombe: It may be fun to theorize about massive attacks on the internet, attacks that would grind it to a halt, leaving us all unconnected … The notion of a "Cyber Pearl Harbor" is worthy of discussion, but the real issue is the use of Internet attacks for more limited purposes. We have had attacks in the past that have cost billions of dollars, put businesses at risk, and put people at risk by hampering potential emergency response. These are in and of themselves significant. The fact that we haven't seen a massive event doesn't mean that we couldn't see it, and if your company lost millions of dollars due to the "I love you" virus several years ago, you probably think this massive attack has already happened!

We need to have a holistic perspective. We need to think of the impact of the loss of some portion of connectivity to the nation, measured in dollars or frustration. Redundancy and alternative routing make a massive impact from an attack less likely. However, a combined physical / cyber attack, for example taking out key nodes with bombs, could have a dramatic impact. The convergence of information and communications means that an Internet attack could mean the immediate loss of voice and data communications—not just a loss of e-mail or access to the Internet.

In the area of cyber reconstitution, roles and responsibilities for government and industry have not been widely established. There is no governance strategy to respond in a coordinated manner to a massive attack. What is the best way to approach this problem? Are current efforts such as the National Response Plan to assign roles and responsibilities adequate?

Lacombe: One has to start with the understanding that the responsibility of CIP is shared by public and private sectors. The private sector doesn't get to duck this responsibility. They have a business requirement to stay in business.

At what point does the Federal government need to step in? One might get a lesson by looking at the telephony side of the house—the National Communications System (NCS) / National Security Telecommunications Advisory Committee (NSTAC) is an excellent collaboration in which government and industry have created a cooperative environment geared toward restoring essential connectivity based on criticality indices, such as emergency communications. As one follows the convergence path--transparency between telephony, voice, and data--the cooperative environment we see on the telephony side of the house would be usable in data / Internet activities as well. I look at the NCS / NCC response to 9/11—as they responded, they didn't ignore data communications requirements. The immediate requirement was for voice, but data communications were not ignored. This may at least be a direction for us to investigate.

The National Response Plan is a step in the right direction. It's not a new idea, but a good step. I am not sure that on the data side we have the kinds of communications / cooperation that we have on the strategic communications side with NCS/NCC and DHS. The cyber side is relatively new in terms of our reliance on it, and if we didn't rely on it for essential activities it wouldn't matter, but as we do, it must be addressed with the same level of seriousness.

The key is still a public / private collaborative approach to reconstitution. However, the government is the only place where you can exert the nationwide leadership to plan for that reconstitution in advance—the government absolutely needs to take the lead here. This must be a collaborative approach, but government needs to lead the thinking,
(Continued on Page 26)

Legal Insights

Fighting the War on Terror in U.S. Courtrooms: A Glance at Major Terrorism Related Cases Since the September 11th Attacks

Colleen Hardy
Legal Researcher, CIP Program

This month marks the five year anniversary of the harrowing events that occurred on September 11, 2001. Since that dark day, there has not been another terrorist attack on United States soil; however, this does not mean that the threat is gone. Quite the contrary, the cases investigated and prosecuted by a mourning, yet determined and proud government, tell a different story.

That the U.S. has not suffered another tragic attack is not due to lack of effort from those who wish us harm. In fact, hundreds of individuals and groups have been arrested and prosecuted in the past five years for planning numerous large scale attacks against the U.S. Additionally, several individuals and groups have been arrested and prosecuted for supporting those who wish to cause us harm.

The first major indictment on terrorist related charges after the 9/11 attacks was against Richard Reid in late 2001, three months after 9/11. Reid, a United Kingdom citizen, attempted to blow up an American Airlines flight he was on from Paris to Miami. He had explosives in his shoes and tried to ignite them, but was apprehended by several passengers on the plane. He was charged with attempted use of a weapon of mass destruction against U.S. nationals outside the U.S. and sentenced to life in prison.

"That the U.S. has not suffered another tragic attack is not due to lack of effort from those who wish us harm. In fact, hundreds of individuals and groups have been arrested and prosecuted in the past five years for planning numerous large scale attacks against the U.S."

Zacarias Moussaoui was also indicted in 2001 and charged with several terrorist related charges. Moussaoui, a French citizen, claimed he was supposed to be on the fifth plane on September 11th. The government also alleged Moussaoui attended flight school in Minnesota and attended an al Qaeda training camp in Afghanistan. After an extensive trial in April 2006, Moussaoui was sentenced to life in prison.

Another well known case was that of John Walker Lindh. Lindh was first apprehended in Afghanistan in November 2001; however, the make-shift prison where he was being questioned was attacked and Lindh escaped. He was recaptured a few weeks later. Lindh, who grew up in California, became known as the "American Taliban." Baptized Catholic, he converted to Islam when he was sixteen and traveled to Yemen when he was seventeen to learn Arabic. The government alleged that he traveled to Afghanistan in the spring of 2001. Lindh accepted a plea agreement with a sentence of twenty years in prison.

In 2002, Earnest James Ujaama was indicted on charges of conspiracy to provide goods and services to the Taliban. The government alleged that Ujaama, a U.S. citizen, transferred funds, and delivered and installed software for the Taliban. Ujaama admitted to operating several websites that solicited donations of money, goods and services to Taliban-sponsored programs. He cooperated fully with the government and was sentenced to two years in prison followed by three years of supervised release.

In 2003, several Northern Virginia and Maryland men were indicted on multiple terrorism related charges and became known as the "Virginia Jihad Network." Their

(Continued on Page 10)

Legal Insights *(Continued from Page 9)*

leader, Ali al-Timimi, was a prominent Islamic scholar and recently received his PhD from George Mason University. The government alleged that al-Timimi encouraged others to travel to Pakistan and train with a militant group called Lashkar-e-Taiba. The government also alleged that the men would meet at local paintball facilities to practice military style shooting to prepare for holy war or jihad. Al-Timimi was sentenced to life in prison. Other member's sentences ranged from fifty-two months to life in prison.

Hemant Lakhani was also charged in 2003. Lakhani was charged with providing material support to terrorists. Lakhani, a UK citizen, met with an undercover FBI agent in New Jersey and attempted to sell him fifty surface-to-air missiles. He told the undercover agent that he knew the purpose of this sale was to shoot down U.S. airplanes and to cause severe economic damage to the U.S. He was sentenced to forty-seven years in prison. Lakhani was sixty-eight years old at the time of his sentencing.

Iyman Faris, a truck driver from Ohio, was also charged with providing material support and resources to al Qaeda. Faris, a U.S. citizen, provided a tremendous amount of support to al Qaeda by researching "ultra light" aircraft for a top al Qaeda official in 2000. Additionally, he informed high ranking al Qaeda officials of his trucking routes to the airports and how much cargo he could carry. And lastly, he provided extensive research on New York bridges and equipment required to take down a bridge. He was sentenced to twenty years in prison.

In 2004, Saajid Mohammed Badat was indicted on charges of conspiring and aiding and abetting Richard Reid. Badat, a UK citizen, researched plastic explosives with Reid and purchased his ticket for a flight to the United States. However, before his scheduled flight, he had a change of heart and e-mailed his associates to explain that he would not go through with his attack. He was tried in the UK and was sentenced to thirteen years in prison.

Shahawar Matin Siraj, a Pakistani citizen, was also indicted in 2004 on conspiracy charges. He and another individual were arrested on the night before the 2004 Republican National Convention carrying crude diagrams of the subway station in Herald Square, the busiest station in New York City. The government alleged that he and his co-conspirator planned to blow up the Herald Square station. He was convicted in May 2006 and is awaiting his sentencing. He faces up to life in prison.

In 2005, Ahmed Omar Abu Ali, a U.S. citizen, was indicted on charges of providing material support to the al Qaeda network, conspiracy to assassinate the President and conspiracy to hijack aircraft. He grew up in Falls Church, Virginia, and after graduating from high school, moved to Saudi Arabia and became a member of al Qaeda. He and another co-conspirator discussed plans to assassinate President Bush. He also discussed creating al Qaeda cells in the U.S. and received *(Continued on Page 26)*

Dear Editors:

I read *The CIP Report* for August 2006 with great interest. In Iowa, we have been working since the events of 9/11 to identify the State's critical infrastructure and key assets. We have also worked to discuss and explore the interdependencies of these structures and assets and are partnering with the business community to advance initiatives and activities to provide for infrastructure and asset protection.

I had the good fortune to sit on two federal advisory committees to help develop the NIPP and the Emergency Services Sector plan. While I agree that the NIPP now provides a strong strategic framework for infrastructure protection through partnership between all levels of government and the business community, I also find that many of the sector specific plans are lacking in their initial efforts. There remains much work to be done in this critical area.

In the Report, I took special note of the article by Mr. Randy Jackson, regarding the role of States in the NIPP. In his article, Mr. Jackson discusses states' power and writes, "An important power reserved to the states is police power. Through their police power, state governments take steps to protect the health and safety of their citizens. Protecting CI/KR assets from acts of terrorism and /or assisting in their recovery in the event of a natural or other type of disaster would fall under this state power."

Mr. Jackson seems to insinuate that infrastructure protection is simply a police powers issue and that while states have no legal obligation to do so, they should cooperate with the federal government in this effort. In turn, the federal government may compel that cooperation by the manner in which they manage grants and provide funding to the states. I would submit that infrastructure goes far beyond issues of police power or the affects of grants funding. Protection of critical infrastructure must look not only from a terrorism perspective, but more importantly from an all-hazards approach that would encompass natural and accidental disasters. It must also take a multi-disciplinary approach encompassing the responsibilities of law enforcement, fire, public health, environmental, agricultural and any number of other officials and influences. There are not only questions of police powers, but also broad policy considerations.

Thank you for your work and that of your staff and contributors on this vital issue of national importance. I look forward to your next Report and thank you for the opportunity to comment.

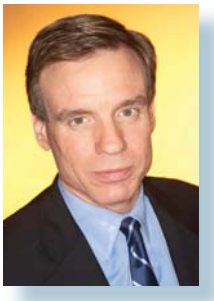
Sincerely,

David L. Miller, Administrator
Iowa Homeland Security & Emergency Management

Op-Ed

To Keep America Safe

Governor Mark Warner



Five years have passed since September 11, 2001 – longer than the duration of the Civil War or World War II. We have made progress, but I don't think Americans can be satisfied. Because five years after 9/11, the American people are safer -- but they are not as safe as they should be.

Since 9/11, the Bush Administration has squandered much of the world's goodwill, dividing our friends, and uniting our enemies. When the 9/11 Commission issued its Report Card on counter-terrorism, there were 5 F's and 12 D's. Our intelligence agencies are still struggling to share information, the FBI has not adjusted to its counter-terrorism mission, and the Department of Homeland Security offers a case study in what happens when people who deplore government undertake radical government reform.

In the face of these failures, this Administration likes to say Democrats have a pre-9/11 mentality. Well, Virginia was attacked on 9/11, and Virginians elected me as the first post-9/11 governor in this country. I met with the firefighters who rushed into the Pentagon and the families of the fallen. And I had to act to protect my people, often while our federal partners were mired in bureaucracy.

Virginia was the first state to create a cabinet-level position dedicated to security and preparedness. We established the Virginia Fusion Center to serve as a focal point for intelligence gathering and information sharing. We built a state-of-the-art Virginia Emergency Operations Center to coordinate our response to a major disaster. We funded an interoperable radio system, so first responders can communicate during a crisis. We bolstered our public health system to respond to a bio-terror threat or major outbreak of disease. And we tapped the civic spirit that followed 9/11 by creating Virginia Corps to allow our citizens to join in preparedness efforts.

Above all, we did not treat the safety of our people as a Republican or a Democratic issue. When somebody came to me with an idea, I didn't check to see if it had an "R" or a "D" next to it, and I worked with our majority-Republican legislature to take actions to protect all Virginians. On a national level, we're not going to get it right if we continue to favor ideology over competence, or fail to tap the American people's will to come together. To keep America safe, it's time for a new approach.

First, Washington has to work. FBI reform must be given new urgency. The Bureau needs to better gather and analyze information, share with other agencies, and move nimbly to keep up with a nimble enemy. And if the FBI cannot do the job, we need a new agency that can. We also need a Director of Homeland Security Intelligence under the Director of National Intelligence who is effectively the "combatant commander" for domestic intelligence – drawing upon and managing information and resources from state and local police, federal agencies, and the private sector to prevent another attack.

Second, we need a fresh approach on the frontlines. From New York to Peoria, all metropolitan areas – regardless of state and local boundaries -- should have protection and response plans. It must be clearly defined who is in charge, and what the role of each agency is, before the next attack – or hurricane. FEMA should be an independent agency, with a direct report to the President, and should work seamlessly with local and state responders. All of our first responders should have interoperable communications. And all major metropolitan areas should have protective gear to respond to attacks with chemical, biological or radiological weapons, as well as a medical surge capacity.

We also need more than first responders – we need 'first preventers.' Local police forces should have the training and capability to gather and share information to prevent attacks. We need metropolitan fusion centers to integrate state and

(Continued on Page 29)

Senate Committee on Homeland Security and Governmental Affairs September 12, 2006 Hearing on Homeland Security

Excerpt from Statement of Steven N. Simon[1] "Priorities for Homeland Security"

(Steve Simon was formerly a CIP Program Senior Fellow and a previous contributor to The CIP Report.*)*

My understanding of the Committee's objectives in holding this hearing is that witnesses should focus on the future and address themselves to issues that might help both Congress and the Executive branch set homeland security priorities. The Committee it seems to me is doing the right thing. Our vulnerability at home to terrorist assault, as well as to natural disasters, is essentially infinite. The fact is that not everything can be protected. Judicious decisions about what to protect given our wholesale and inevitable exposure to attack by clever and disciplined terrorists are essential.

What follows are my personal reflections on this vexing problem. Given the myriad threats to our infrastructure – critical and otherwise – and to the lives of our fellow citizens, other analysts will legitimately come to different conclusions about the best way to focus our collective efforts and especially those of the agencies under the jurisdiction of this committee, and of departments and agencies with which DHS must interact continuously and cooperatively in order to fulfill its daunting mandate.
I will concentrate on three issues: first, the importance of cities as terrorist havens and terrorist targets; second, the continuing significance to many jihadists of weapons of mass destruction (WMD); and third, the need to preserve the good will and sense of belonging of America's Muslim communities as a matter of national security, beyond the intrinsic virtues of a cohesive, considerate society in which citizens of all creeds can feel at home.

Urban Warfare

The jihad that has evolved since September 11th has become a war of cities. The transition from caves to condos, as one observer described this evolution, is impressive. Although the relatively remote, rural bases that incubated the jihad had strong advantages, especially given the centrality of social networks to the early jihad, municipalities have their own attractions. They offer anonymity, but also community, both of which can confer a kind of cover. Urban neighborhoods, with their numberless apartments, coffee-houses, mosques and Islamic centers, provide the setting for recruitment, clandestine meetings, preparation of weapons and other activities that form the terrorist enterprise. Moreover, the majority of urban areas in which jihadists have established a presence are not targets for air strikes, Hellfire missiles, or submarine-launched cruise missiles. Think of Muhammad Atta's Hamburg, or the Leeds of Muhammad Siddique Khan, orchestrator of the 7/7 bombings of the London underground and bus systems. Post-bin Laden jihadists are not the first militants to avail themselves of these tactical conveniences. The radical campaign in Egypt that began in mid-1970s was spawned in Cairo, one of the world's largest cities. And of course non-Muslim terrorist organizations, such as the Provisional Irish Republican Army (IRA), have long thrived in urban areas. It could be said that having adapted to city life, the jihad has really come into its own.

Qualities that favor the jihadists' defensive requirements do not tell the whole story. The other side is that cities are where their targets – both symbolic and of flesh-and-blood – are to be found in abundance and proximity. There are many aspects of Islamist militancy that are quintessentially modern. The transformation of cities into fields of jihad is a classic example of the movement's modernity. It is part and parcel of the post-World War II process of urbanization that swept the Middle East, North Africa and Pakistan. Large-scale migration of Muslims to Europe represents perhaps the last phase of this urbanizing process. In these cities, Muslims radicalized by a potent combination of powerful imagery in the media, socio-economic exclusion, and a set of simple, but internally consistent religious and ideological concepts, have ample targets for their hunger for retribution and duty – from their perspective – of self-defense. One of the striking features of contemporary Muslim public opinion to emerge from recent Pew polls is the degree to which Muslims in far-flung, diverse places have come to see themselves as having "more in common nowadays."
(Continued on Page 22)

[1] Full transcript available at: http:// http://hsgac.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=394

Excerpt from Statement of Richard A. Falkenrath[1] Deputy Commissioner for Counterterrorism New York Police Department

The NYPD Counterterrorism Program

The NYPD is charged with the protection of New York City. With a population of over 8.1 million and an area of 321 square miles, New York is the largest city in the United States. New York is also the most densely populated major city in North America as well as one of the most diverse: an estimated 40 percent of the population of New York City is foreign born. The New York metropolitan area has a population of 18.7 million, making it one of the largest urban areas in the world. New York City is an international center for business, finance, media, culture, diplomacy, tourism, and travel. In 2004, the of the New York urban area was estimated at $901.3 billion, a level greater than all but about a dozen countries in the world.

With a staff of over 52,000 people and an annual budget of $3.8 billion, the New York Police Department is the largest public safety agency in the United States and one of the largest police departments in the world. (For comparison, the NYPD is larger than the U.S. Coast Guard and more than twice the size of the Federal Bureau of Investigation; at the federal level, only the Army, Navy, Air Force, and Marine Corps are larger.) Over 1,200 NYPD personnel are members of the National Guard or the Reserves; more than 800 have served or are serving in Iraq.

Every American remembers the heroism and sacrifice of New York City's first responders – from the Fire Department of New York, the Port Authority Police Department, the NYPD, and many other agencies on September 11, 2001. I can claim no credit for their heroism and sacrifice – at the time of the attacks, I was working in the relative safety of the White House – but I serve now with the knowledge that my present-day colleagues lost family and friends that day and risked their own lives, and will do so again if we are attacked once more.

Needless to say, since the terrorist attacks of September 11, 2001, the NYPD has enhanced its counterterrorism program in a manner that is unique in this country. The New York Police Department has made the defense against the terrorist threat its number one priority.

Threat and Vulnerability Reduction

The NYPD created a threat reduction and infrastructure protection program. Critical infrastructure is divided into five categories, and a team of investigators covers each one. These officers visit facilities throughout the City, identify vulnerabilities, and develop comprehensive protection plans with site managers. Members of the Counter Terrorism Bureau have conducted hundreds of threat and vulnerability assessments of strategic and high-visibility sites. The goal of these assessments is to work with the private sector and other city agencies to improve the security of their facilities against terrorist attacks.

Outreach to the Private Sector

Under Operation Nexus, members of the NYPD Intelligence Division meet with small business owners and suppliers throughout the city who might unwittingly be used to provide material support to terrorists. Our goal is to increase their counterterrorism awareness. We ask them to report anomalies in purchases of goods and specialized rental equipment to our citywide counterterrorism hotline.

In July 2005, the NYPD launched a new initiative with the private security industry in New York called "NYPD Shield." We have created a comprehensive program website featuring training materials and threat updates, and we have offered detailed briefings to a number of private sector industries. We exchange threat information daily with the city's corporate and institutional security directors though an instant messaging system. NYPD has also held briefing sessions for various segments of the public who may come in contact with terrorist plotters.

Counterterrorism Training

NYPD has also provided training to all of our uniformed personnel in the new Citywide Incident Management System (CIMS). The system provides for a command structure that allows the Police Department to work seamlessly with other first responders, as ideally envisioned in the National Response Plan.

The result of our significant training activity is that New York City has never been better prepared to defend itself from a terrorist threat. These preparations, however, come at a steep price: about $178 million per year to maintain our daily counterterrorism and intelligence activities. I want to empha-

(Continued on Page 24)

[1] Full transcript available at: http:// http://hsgac.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=394

Protecting the Homeland Post September 11

Department of Homeland Security Fact Sheet

The Department of Homeland Security (DHS) has taken significant action to improve the nation's security since the terrorist attacks of September 11, 2001. By improving security measures for the nation's aviation system, implementing measures designed to protect our critical infrastructure, using biometrics to establish and verify identity, strengthening border security, reflecting the lessons-learned from Hurricane Katrina, increasing the nation's preparedness for a disaster, and enhancing information sharing among federal, state, local, and international partners, DHS is leading the effort to protect the homeland.

Securing the Nation's Transportation System

The Transportation Security Administration (TSA) has established a comprehensive, layered security approach to protecting our nation's aviation system – including hardened cockpit doors, additional Federal Air Marshals, explosive screening devices and 100% screening for all passengers and checked baggage by a professionally trained workforce – enabling our response to be as flexible, dynamic, adaptable and unpredictable as the enemy we face. Further research is ongoing and new technologies are being developed, tested and deployed to improve aviation, port, rail, bus and mass transit security while focusing resources where the risk is greatest.

Training Personnel in Advanced Methods to Detect Explosives and Deter Other Serious Threats:

DHS provides more than 43,000 Transportation Security Officers (TSOs) at over 700 airport security checkpoints and 7,000 baggage screening areas. With nearly 38,000 TSO's trained in the detection of explosive materials and devices, 425 Explosives Detection Canine Teams active in 80 airports nationwide (representing a 70% increase since 2003), Visible Intermodal Protection Response (VIPR) teams deployed to supplement existing security resources, and thousands of Federal Air Marshals protecting U.S. flights, these layers of security are helping to ensure the safety of the traveling public and prevent any terrorist or criminal activity.

Deploying New Technologies to Improve the Screening of Passengers and Baggage

Approximately 4,000 metal and x-ray detectors are present at 440 airports within the United States to check passengers for harmful materials or weapons that may pose a threat to aviation security. Since 9/11, TSA has also deployed 1,200 Explosive Trace Detector machines to passenger screening checkpoints.

100% of Checked Baggage Now Undergoes Screening

On 9/11, five percent of checked baggage was screened. Whether checked or taken as a carry-on, TSA now screens 100% of all checked baggage utilizing enhanced technology that quickly determines whether a bag contains a potential threat to aviation security.

Securing Air Cargo with a Layered Security Solution

While promoting the free flow of commerce, DHS has employed a risk-management approach designed to strengthen security across the spectrum of cargo, conveyances and people utilizing different detection methods including enhanced technology, human inspection, and canine teams. TSA has enhanced shipper and supply chain security by pinpointing cargo deemed an elevated risk through prescreening, targeted inspections, and stronger security measures at cargo facilities. DHS is now conducting Air Cargo Explosives Detection Pilot Programs to test ways additional cargo can be screened prior to loading on passenger aircraft.

Background Checks for Truckers Hauling HAZMAT

DHS has checked more than 2.7 million truckers against terrorist watch lists and more than 200,000 persons receiving new licenses or renewing their old commercial driver's licenses. As of August 2006, drivers licensed in Canada or Mexi-

(Continued on Page 15)

Protecting the Homeland *(Continued from Page 14)*

co must also undergo a background check as part of CBP's Free and Secure Trade (FAST) program before transporting placarded amounts of hazardous materials in the U.S.

Protecting the Nation's Critical Infrastructure

Since 9/11, DHS has taken significant steps to protect our nation's critical infrastructure and key resources, including our nation's ports, rail, and mass transit systems. DHS has increased screening of inbound cargo, forged new international partnerships to create global standards in supply chain security, and awarded hundreds of millions of dollars to enhance security and protect our nation's infrastructure systems.

Strengthening Port Security

The U.S. Coast Guard created port security teams to assess over 60 strategic port locations. USCG also completed special assessments on several classes of vessels including ferries, LNG vessels, certain dangerous cargo barges and single skin tank vessels. The Coast Guard also developed the port security risk assessment tool to assess and establish risk-based profiles. With the President's FY 2007 Budget request, total DHS funding for port security activities since FY 2004 total nearly $10 billion.

Developing the Transportation Worker Identification Credential

DHS is elevating security at our nation's ports by requiring a biometric identification card or Transportation Worker Identification Credential (TWIC) and background check for those individuals requiring daily access to these critical facilities. Extensive background checks have already been completed on over 400,000 port workers. The credential includes a more extensive background check and ensures port workers and vessel operators are fully vetted before they are able to access secure areas.

> "So looking back and looking forward, how do we build on our progress to date? What are the remaining challenges we have to face? And how are we going to allocate priorities among them? And what is the path we have to follow to achieve those steps that must be in place to guarantee ourselves and our families safety in the years to come?
>
> Well, let me say, there's one critical thing we have to recognize at the threshold. We have to be focused on the most significant risks, and we have to apply our resources in the most practical way possible to prevent, protect against, and respond to man-made and natural hazards. That means we have to make a tough-minded assessment, and we have to recognize that it is simply not possible to eliminate every threat to every individual in every place at every moment. That is simply not the way life works."
>
> -Secretary Michael Chertoff on 9/11: Five Years Later

Over $1.1 Billion Has Been Provided to Protect Critical Infrastructure

Through programs designated for infrastructure protection, DHS has provided more than $1.1 billion to date to strengthen the nation's ability to prevent, protect against, respond to and recover from terrorist attacks, major disasters and other emergencies that could impact this country's critical infrastructure. By the end of September, DHS will award approximately $373 million more funding for these purposes. These grants are distributed through seven specific programs that allocate funding toward transit security (rail, bus, and ferry systems); buffer zone protection surrounding chemical facilities, nuclear and electric power plants, dams, stadiums, arenas and other high-risk areas; intercity passenger rail operations; our nation's highways; and critical port infrastructure.

Infrastructure Protection Grants

These grants consider threat, vulnerability and consequences, and recognize the unique characteristics of our nation's seaports, transit systems and other critical infrastructure assets. The FY 06 programs *(Continued on Page 16)*

Protecting the Homeland *(Continued from Page 15)*
included: $9.5 million for the Intercity Bus Security Grant Program; $4.8 million for the Trucking Security Program; over $168 million for the Port Security Grant Program; over $7.2 million for the Intercity Passenger Rail Security Grant Program; nearly $136 million for the Transit Security Grant Program; nearly $48 million for the Buffer Zone Protection Program; and $25 million for the Chemical Sector Buffer Zone Protection Program.

Nearly $110 Million Awarded To Major Rail Systems in 2006

This year, the eight largest mass transit rail systems in the country have been awarded $103 million in security grant assistance. Eligibility announcements for further awards have been made and final grant awards to these systems will be made later this year, bringing the total to roughly $110 million. To date, DHS has provided nearly $375 Million to the Nation's Mass Transit Systems.

Rail Security Pilots

Through S&T's Rail Security Pilot (RSP), DHS field tested the effectiveness of explosives detection techniques and imaging technologies in partnership with the Port Authority of New York and New Jersey. In April 2006, TSA conducted the Mobile Security Checkpoint (MSC) pilot with MARC and Maryland Transit Administration to screen commuter rail passengers and their bags for explosive material. The MSC pilot was conducted to determine the operational feasibility, effectiveness, and the suitability in a transportation environment of commercially available screening technology installed in a mobile container. The results from this pilot will be used to determine if such a container could be used for screening in the transportation environment, or possibly in others.

Providing a Coordinated Approach to Critical Infrastructure Protection

Through the National Infrastructure Protection Plan (NIPP), DHS has established a comprehensive risk management framework that clearly defines the roles and responsibilities among government, private industry, nongovernmental agencies and other key partners in protecting our nation's critical infrastructure, enhancing additional security measures and focusing resources according to risk. Seventeen Sector-Specific Plans that complement the NIPP and detail the risk management framework will be released in December 2006. These plans will address unique characteristics and risk landscapes, will be developed in collaboration with sector specific security partners, and include such areas as agriculture and food; energy; public health and healthcare; banking and finance; drinking waters and water treatment systems; information technology; telecommunications; postal and shipping; transportation systems including mass transit, aviation, maritime, ground or surface, and rail and pipeline systems; chemical; commercial facilities; government facilities; emergency services; dams; nuclear reactors, materials and waste; the defense industrial base; and national monuments and icons.

Strengthening Border Security

On September 11, 2001, the nation lacked a comprehensive multi-agency strategy for securing our borders and enforcing our immigration laws. DHS has taken significant steps to prevent terrorist and criminal activity from entering the U.S. by unifying personnel and law enforcement responsibilities at our nation's borders, ports of entry and between ports of entry; strengthening our deployment of personnel, infrastructure and technology to detect and prevent certain threats; and establishing uniform standards for document authentication and verification that enable government officials to make real-time decisions regarding the admissibility of those attempting to travel or enter the U.S.

Screening Visitors to the U.S. Against Watch Lists and Criminal Records

The US-VISIT program uses advanced biometric technologies to screen visitors to the U.S. against various watch lists to prevent terrorists from entering the country. To date, US-VISIT has been deployed to 116 airports, 15 seaports, and 154 land ports of entry and processed more than 61 million people applying for admission at U.S. ports of entry. Nearly 1,200 criminals and immigration violators have been intercepted at entry into the United States based on the biometric information alone. DHS and CBP also deployed the Inte-
(Continued on Page 17)

Protecting the Homeland *(Continued from Page 16)*
grated Automated Fingerprint Identification System to all 142 Border Patrol stations and more than 150 ports of entry. This technology has enabled CBP to identify hundreds of homicide, kidnapping, robbery and sexual assault suspects as well as thousands of other wanted individuals. Moreover, U.S. Citizenship and Immigration Service conducts approximately 135,000 background checks on applicants seeking immigration benefits each day.

The Student and Exchange Visitor Information System (SEVIS)

SEVIS was implemented in January of 2003, and is a web-based system that provides real-time, up-to-date information on F, M and J visa holders that can be accessed electronically. It is an effective tool used by law enforcement to ensure that foreign students and exchange visitors in the United States are complying with the terms of their immigration status and are not a threat to national security. Prior to SEVIS, there was a decentralized, manual, paper-driven process that monitored foreign students attending more than 70,000 schools. Today, SEVIS enables over 8,600 schools and 1,400 exchange visitor programs in the United States to host over 800,000 foreign students and exchange visitors.

Increasing Manpower and Resources

Since President Bush took office, the number of Border Patrol agents has increased from 9,000 to more than 12,000, and will double to 18,000 by the end of 2008. CBP officers at our U.S. ports of entry have increased 50 percent and funding for border security efforts has risen by 66%. The number of ICE investigators has grown 25%, funding for interior enforcement has risen 42%, and the number of ICE fugitive operations teams has grown from 17 to 45 nationwide. Since March 2003, these teams have arrested more than 52,000 illegal aliens, including roughly 22,000 of who had criminal records.

Increased Resources toward Securing the Border

In 2005, DHS established the Secure Border Initiative (SBI) to strengthen security along our nation's borders through increased manpower and resources, new technologies and enhanced immigration enforcement. Under SBI, DHS has expanded the practice of expedited removal which substantially reduces the amount of time an illegal migrant spends in processing before being returned to their home country; established fencing and barriers to improve security along the border; and will harness cutting-edge technology through SBInet - an integrated effort combining the latest detection technology with new infrastructure investments that will greatly increase our border enforcement capabilities.

Ending "Catch-and-Release"

DHS has effectively ended the practice of "catch-and-release" along the southern and northern borders for other-than-Mexican populations by enforcing a catch-and-remove policy. The President's FY '07 budget proposes increasing the number of beds in detention facilities to 27,500. In addition, $257 million has been approved which will add 4,000 beds this year; while 500 beds were added in Willacy County, Texas in less than 45 days. With expanded bed space and decreased processing times under the Secure Border Initiative, DHS is strictly enforcing this "catch and remove" policy enabling us to detain all non-Mexican illegal immigrants apprehended along the southern and northern border until they can be returned to their home countries.

Deploying the National Guard in Operation Jump Start

Since May 2006, the Administration has leveraged the support of up to 6,000 National Guard to help keep the border safe while additional Border Patrol agents and new technologies are brought online. Their support has freed up more than 380 Border Patrol agents for frontline duty and assisted with more than 6,700 illegal alien apprehensions and the seizure of approximately 34,000 pounds of marijuana and 1,700 pounds of cocaine since the start of the Operation.

ICE Worksite Enforcement

In FY 2004, Immigration and Customs Enforcement initiated 460 investigations; there were 79 indictments and 87 convictions. These numbers increased in FY 2005 to 502 investigations, 186 indictments and 160 convictions, and in FY 2006 (as of August 22) there were 1097 investigations, 184 indictments and 177 convictions.

Development of e-Passports

In coordination with the State
(Continued on Page 18)

Protecting the Homeland *(Continued from Page 17)*

Department, DHS is providing technological solutions, such as the e-passport, to improve the travel process and enhance fraud detection. E-Passports effectively eliminate passport fraud and serve as an example of international cooperation to ensure safe travel.

Increasing Emergency Preparedness

On September 11, 2001, the nation lacked an integrated incident management system, had done little catastrophic planning, and had no means by which relief supplies could be tracked in the event of a disaster. DHS has dramatically strengthened the nation's preparedness for a disaster by awarding billions in grant dollars; building new relief supply systems; assessing disaster plans for states, territories, and major urban areas; and creating a national plan for incident response.

$18 Billion Has Been Awarded to State and Local Governments to Increase Their Level of Preparedness

Since the creation of the department, approximately $18 billion has been awarded to state and local governments for equipment, training, exercises and various other measures designed to increase the level of security in communities across the nation.

Strengthening Interoperability Communications and Capabilities

Since 2003, DHS has provided over $2.1 billion to states for interoperable communications equipment, planning, training, and exercises. Through the Interoperable Communications Technical Assistance Program, DHS has provided onsite assistance to improve interoperable capabilities in more than 75 states, urban areas, and metropolitan regions. Through the Department's RapidCom initiative, first responders and incident commanders in ten high-threat urban areas now have the ability to communicate with each other and their respective command centers in the event of a large emergency incident like a terrorist attack. These cities include: Boston, Chicago, Houston, Jersey City, Los Angeles, Miami, New York, Philadelphia, San Francisco, and Washington, DC. To further assess the capacity for communications interoperability among law enforcement, fire, and emergency medical service first responders in all 50 States and DC, DHS initiated the National Interoperability Baseline Survey which will result in a public score card that will identify gaps and help us to determine improvements needed to be made in the near term. A final report for the Baseline Survey is planned for October 2006.

National Response Coordination Center

With the new state-of-the-art National Response Coordination Center (NRCC), the federal government can proactively and quickly provide federal support to states and communities to ensure critical life-saving assistance and incident containment capabilities are in place to respond quickly and efficiently to catastrophic incidents. The NRCC at FEMA coordinates the national-level response to any natural or man-made incidents. The NRCC monitors potential or developing incidents and supports the efforts of regional and field components, including coordinating the preparedness of national-level emergency response teams and resources; in coordination with Regional Response Coordination Centers, initiating mission assignments or reimbursable agreements to activate other federal departments and agencies; and activating and deploying national-level specialized teams. Using advanced technology, the new NRCC brings together teams of emergency response professionals from federal agencies and the private sector.

Increasing Situational Awareness through the Common Operating Picture

Activated in May 2006, the Common Operating Picture (COP) is a display of relevant information that is derived from a Common Operating Database (COD) and shared by several agencies and organizations. The COP/COD system is a situational awareness tool that can be modified for the strategic, operational and tactical levels and is active in the National Operations Center (NOC). As part of an incrementally phased development effort, the DHS COP/COD system has focused on the 2006 hurricane season and has been implemented in selected DHS offices and component and inter-agency operation *(Continued on Page 19)*

Protecting the Homeland *(Continued from Page 18)*

centers. Subsequently, the COP/COD system will be implemented nationwide for all Homeland Security partners, for all hazards, and for all threats.

DHS Reviewed 131 State and Local Emergency Plans

By reviewing state and local disaster plans, collocating decision-makers, and pre-designating federal leadership, DHS is improving coordination across all levels of government. Through the National Plan Review, DHS completed visits to 131 sites (50 states, 6 territories, and 75 major urban areas) and reviewed the disaster and evacuation plans for each. These reviews will allow DHS, states, and urban areas to identify deficiencies and improve catastrophic planning.

Established The National Response Plan (NRP)

The NRP established a unified, all-discipline and all-hazards approach to enhance the ability of the United States to manage domestic incidents through the alignment of Federal coordination structures, capabilities and resources. The NRP and its coordinating structures and protocols provide the mechanisms for the coordination and implementation of a wide variety of incident management and emergency assistance activities.

Ready Campaign

Launched in February 2003, Ready is a national public service advertising campaign produced by DHS and the Advertising Council to educate and empower Americans to prepare for and respond to emergencies including natural disasters and potential terrorist attacks. The campaign, which includes information for individuals, families, Spanish speakers and businesses, distributes its messages through public service advertisements, brochures, web sites, a toll-free phone line and partnerships with a wide variety of public and private sector organizations. The Ad Council has declared Ready one of the most successful campaigns in its more than 60-year history. Ready has generated more than $568 million in donated media support; more than 1.9 billion hits and 23.8 million unique visitors to www.ready.gov; and more than 7.4 million Ready materials have been requested or downloaded from the Web site. Additionally, Citizen Corps, a component of USA Freedom Corps and coordinated by DHS, was created to help coordinate volunteer activities that will make communities safer, stronger, and better prepared to respond to any emergency situation. There are currently over 2,000 Citizen Corps Councils reaching 72% of the population and operating in all 50 states and 6 U.S. territories. At the state and local levels, grants totaling more than $107 million help implement the Citizen Corps programs.

Improving Information Sharing

The events of September 11, 2001 exposed the importance of information sharing across all levels of government and throughout the international community. DHS has established new mechanisms to collect and share vital information across various sectors, and has provided support to local communities.

Federal Support for State Fusion Centers

DHS is supporting state and local authorities by providing analysts and direct support to established Fusions Centers which are working toward the common goal of blending relevant law enforcement and intelligence information analysis and coordinating security measures to reduce threats in their communities. To date, DHS has provided more than $380 million to state and local governments in support of these centers and will continue to deploy tailored, multi-disciplinary teams of intelligence and operational professionals to Fusion Centers nationwide with plans to have personnel at all of the major centers by the end of fiscal year 2008. The Homeland Infrastructure Threat and Risk Analysis Center is another tool the department is utilizing to improve information sharing between the federal government and state and local partners by developing three new product lines tailored to meet the intelligence needs of the private sector and state and local governments, including sector-specific documents, unclassified communication with the private sector and quarterly suspicious activity reporting analyses.

Improving Information Sharing to Prevent Terrorists From Boarding Planes

In order to help identify potential high-risk travelers earlier, increase the security of international flights *(Continued on Page 20)*

Protecting the Homeland *(Continued from Page 19)*
to and from the U.S. and alleviate turn-backs and diversions of aircraft, DHS has a proposal to implement the pre-departure transmission of Advance Passenger Information System (APIS) data which provides officers with pre-arrival and departure manifest data on all passengers and crew members. Also, the Office of Screening Coordination oversees the integration of the department's terrorist and immigration-related screening efforts, creates unified screening standards and policies, and develops a single redress process for travelers.

Increased Information Flow among DHS and Federal, State, and Local Partners

DHS communicates in real-time to its partners by utilizing the internet-based Homeland Security Information Network (HSIN). System participants include governors, mayors, Homeland Security Advisors, state National Guard offices, Emergency Operations Centers, First Responders and Public Safety departments, and other key homeland security partners.

Preventing Weapons of Mass Destruction

The threat of weapons of mass destruction is one of the foremost priorities of the Department. Countering the threat of chemical, biological, radiological and nuclear weapons in the hands of terrorist organizations is the gravest danger facing America.

Assessing 100% of Cargo Entering the Country

The National Targeting Center (NTC) provides tactical targeting and analytical research support for Customs and Border Protection (CBP) anti-terrorism efforts and currently assesses information relating to all U.S. bound cargo in order to identify, inspect and reject potentially high-risk cargo before it can enter the United States. Experts in passenger and cargo targeting at the NTC operate around the clock using tools like the Automated Targeting System (ATS) to determine any potential national security risk before entering the U.S.

Scanning 98% of Cargo in our Seaports by the End of 2008

Prior to 9/11, approximately 2 percent of cargo was screened, and virtually none was screened for radiation. There are now approximately 267 Radiation Portal Monitors (RPMs) currently deployed at our nation's seaports and 14,000 handheld detection devices are currently in use. By the end of 2006, 75 percent of seaborne cargo will be scanned by RPM. By the end of 2008, that number will increase to 98 percent.

Establishing the "Global Standard" for Cargo and Port Security

DHS established the Container Security Initiative (CSI) post 9/11 to inspect high risk containers before they are loaded on board vessels destined for the U.S. By the end of this year, more than 50 ports, accounting for over 90 percent of maritime containerized cargo shipped to the U.S., will be part of the initiative. DHS also partners with more than 5,800 global businesses through the Customs-Trade Partnership Against Terrorism (C-TPAT) in which business take necessary steps to improve supply chain security and agree to pre-screen all cargo before entering the U.S.

Domestic Nuclear Detection Office Progress

Post 9/11, the Domestic Nuclear Detection Office has completed the first ever global nuclear architecture, announced contract awards for new radiation detection technologies; completed performance testing for mobile, handheld, backpack, and portable radiation detectors (PRDs) detection systems; and issued broad agency announcements for transformational research and development.

Next-Generation Radiation Portal Monitors

DHS has awarded contracts for the production of next-generation RPMs. A limited number of units will be tested at ports of entry over the next six to nine months. The Advanced Spectroscopic Portal (ASP) Program will be initiated with a purchase of 80 Standard Cargo portals. From this total, each of the three companies awarded contracts for the program will supply portals for testing, spiral development, primary and secondary screening at operational land crossings and seaports.
(Continued on Page 21)

Protecting the Homeland *(Continued from Page 20)*

Training for Law Enforcement and First Responders

DNDO has worked with the Office of Grants and Training (G&T) and the Counter Terrorism Operation Support Team to develop and deliver preventive radiological/nuclear detection training to over 300 law enforcement and first responders at three training sites in New York, South Carolina and Pennsylvania.

Increasing Defenses against Biological Threats

Since 9/11, DHS has significantly strengthened the nation's defenses against biological threats by developing and deploying a network of biological sensors; establishing new facilities to monitor, test and detect potential biological threats; and utilizing new risk assessment tools to inform investments and potential threats.

Detecting and Preventing Biological Attacks

DHS, in partnership with the Environmental Protection Agency (EPA) and the Department of Health and Human Services (HHS), has deployed the first ever bioaerosol monitoring system to more than 30 major metropolitan areas in order to provide early warning of an attack and enable quick and accurate response. The BioWatch system is currently undergoing expansion in the top threat cities to enable detection of smaller amounts of bio-agents, better define the affected areas in the case of a release, and provide increased coverage of critical facilities such as transportation networks.

Established National Biosurveillance Integration System

A 24/7 operation, the National Biosurveillance Integration System is designed to provide early recognition of biohazards of potential national significance and to form a common operating picture through all source reporting relating to all types of public health threats.

National BioForensics Analysis Center (NBFAC)

DHS, in partnership with the Federal Bureau of Investigation (FBI), established the National BioForensics Analysis Center (NBFAC) in 2004 at Ft. Detrick, MD. Utilizing state-of-the-art detection technologies combined with rigorous chain-of-control procedures to analyze samples in secure, contamination free, bio-containment laboratories, this center serves as the lead federal facility to conduct and facilitate forensic analysis and interpretation of materials recovered following a biological attack.

Creating New Centers of Excellence

DHS, in partnership with the U.S. Department of Agriculture (USDA) has established two agricultural Centers of Excellence. The National Center for Foreign Animal and Zoonotic Disease Defense (FAZD) Center of Excellence is actively engaged in research efforts to protect pre-harvest agricultural targets from deliberate or intentional incursions of pathogenic microorganisms responsible for such diseases as Foot and Mouth Disease, Rift Valley Fever, brucellosis, and avian influenza. The National Center for Food Protection and Defense (NCFPD) Center of Excellence is dedicated to developing technologies and understanding the complexities of safeguarding our Nation's food supply chain. ❖

Simon Testimony *(Continued from Page 12)*

This attitude can be seen at work in the United Kingdom, Spain, Germany, The Netherlands and Denmark. Events far removed geographically from these countries, especially developments in Iraq, have mobilized youth in each of their capitals.

The implications of this analysis are, first, that community policing and extensive video surveillance probably need to be stepped up. In this kind of urban warfare, intelligence is acquired best by those who are most familiar with the terrain: police officers walking their beat. On the front line, they get to know their neighborhoods, the residents and the shopkeepers, form and cultivate relationships with local citizens, and develop a sense of the natural order of things and therefore of signs that something is out of the ordinary or warrants investigation. The pivotal role of local law enforcement is reinforced by the incapacity of federal authorities to gather information skillfully, discretely, effectively, and without alienating potential sources of intelligence. The FBI, in particular, presently lacks the numbers, skills, knowledge base and orientation to contribute.

This does not mean however that local law enforcement can or should operate in a vacuum, especially in light of connections that have been disclosed between the self-starter groups in the U.K. and al-Qaeda figures in Pakistan. On the contrary, local police need an umbilical connection to national intelligence agencies in order to connect the dots they're collecting on the ground. It is worth noting that the success of the UK counterterrorism effort in Northern Ireland was largely due the tight linkages between the local police, national police, and Britain's domestic intelligence agency that were forged early in the conflict. Yet information sharing, which all parties claim to be essential, has not advanced significantly. In part this seems to be due to a lack of leadership, and in part to a slow pace of work that seems incommensurate with the urgency of the threat. Thus, issuance of U.S. government sponsored clearances for local police officers, the necessary first step toward sharing intelligence information, has lagged. Even the New York Police Department (NYPD), which has built a very aggressive intelligence collection program and uncommonly close ties to Washington intelligence agencies, has only about 350 cleared officers, or less than one per cent of the force. Many of these patrolmen and detectives have clearances via their status as military reservists rather than as police officers. Countrywide, cleared personnel are usually the handful of detailees to the local Joint Terrorism Task Force. The circle clearly needs to widen.

The other dimension to this issue is the apparent substitution of quantity for quality as Washington's criterion for information sharing with local law enforcement. This puts municipal authorities in the worst of both worlds. The information does not help them do their jobs better, while the sheer volume of unhelpful information can make it harder to manage their responsibilities.

The bigger question, however, is where these police officers will come from, at a time when State, local and federal budgets are under severe pressure. In the upcoming federal budget cycle the COPS program is again under pressure to be cut. This program has put more than 100,000 new police officers on the street over the last decade. Instead of eliminating this program it should be revamped to create the local intelligence capacity cities need.

WMD

Amid growing concerns about the vulnerability of ground transportation, civil aviation, financial institutions and landmarks to large bombs, one should not lose sight of the chemical, biological, radiological and nuclear threats. As many experts have usefully pointed out, jihadists, like other terrorists, prefer tried-and-true methods and shy away from technical innovation. This is certainly true as a general proposition, despite important exceptions, from the first use of dynamite by anarchists early in the 20th century to the experimentation with stabilized liquid explosives by Ramzi Ahmed Yousef in 1995.

The social and economic effects would obviously be proportional to the damage, but the baseline for these effects would be high. Thus, most experts believe that if such a weapon is used it is unlikely to cause mass casualties. Nevertheless, even an attack that took relatively few lives would have an emotional and psychological impact that could tear the fabric of our society and undermine the social contract between government and society. It would also have sizable, perhaps open-ended economic costs, especially if the attacks were repeated or authorities could not assure citizens that the attackers had all been captured or killed. The implication here is twofold. First, Washington must make consequence management a priority. This means not only allocating appropriated funds, but also establishing a high, federally defined performance standard that cities would have to meet reasonably swiftly. The reason for this emphasis on consequence management is simply that a well-planned attack will be difficult to prevent without an uncommon dose of good luck. This being the case, the surest way to stave off the worst emotional, political and economic damage is to show not only the victimized community, but also the American public that the effects of the attack are being handled with confi-

(Continued on Page 23)

Simon Testimony *(Continued from Page 22)*
dence and competence by local and federal authorities working quickly and smoothly – and in lockstep.

The other implication is that Washington and local leaders must begin soon to educate the public about the kind of CBRN attacks that are likely to occur. The purpose is not to scare people. Rather, it is to ensure that Americans understand that for the foreseeable future, a CBRN attack will not necessarily equate to instant annihilation, that it is likely to kill or wound relatively small numbers, and that the federal government and local authorities are prepared for such an eventuality. This is easier said than done, owing to the non-trivial risk that terrorists acquire a weapon capable of a catastrophic nuclear yield. An educational initiative would have to acknowledge this possibility, even as it strove to counter the effect of the Katrina aftermath on public confidence in the competence of their government.

As part of this effort, dedicated broadcasting channels should be set up so that authorities can communicate with the public throughout a crisis and so that the public knows exactly how to "tune-in" to this source of information and guidance. Given the plethora of electronic media and the scarcity of bandwidth, operationalizing this recommendation will not be easy. In a crisis, however, we will wish we had it available.

It goes without saying that the trans-attack and post-attack message must be fully coordinated among federal state and local agencies. It will be just as vital for all these players to have decided beforehand who will be empowered to speak publicly and about what. In the absence of such discipline, the public will be awash in contradictory and inconsistent statements and quickly conclude that no one is in charge. This perception will fuel the panic and desperation latent in what will be a terrifying and unprecedented situation.

Muslim-Americans

The 9/11 disaster showed that skilled, self-possessed and highly determined attackers could do tremendous damage to the homeland without having to rely on a support network within the United States. Halting and uneven progress on border security, especially at airports, has reduced the probability of this sort of attack by injecting uncertainty into terrorist calculations of their chances of getting in. Deterrence at that level does seem to work.

This type of attack, however, is not the adversary's sole option. Other approaches do require infrastructure, in the shape of cells that may or may not be linked to outside networks. A glance toward Western Europe, where this phenomenon seems to be well established, raises questions about circumstances here at home.

Finally, the Madrid and London bombings only confirm that governments need to understand the campaign against transnational Islamist terrorism as an internal security problem to a much greater extent than they have so far. The current approach, however, has been simply to enforce a zero-tolerance immigration policy with respect to the Muslim community. This dispensation has the doubly perverse quality of being both ineffective in counter-terrorism terms and alienating with respect to Muslim Americans. Domestic law enforcement's ranks should also include more Muslims, both to improve the FBI's understanding of and links with Muslim communities and to give Muslims a sense of ownership of America's security challenges. American Muslims do not remotely pose the domestic threat that European Muslims do. To ensure it stays that way, they need to be embraced – not spurned.

I put this issue before the committee for lack of a better place. The challenge outlined here requires leadership and a program. Yet given the way our government is structured, there is no obvious lead agency, or special assistant to the President on the National Security Council or Homeland Security Council, to formulate a program or provide the leadership. We are not the first to face this conundrum. Several years ago, in the wake of a Whitehall study showing upwards of 10,000 al Qaeda supporters in Great Britain, Her Majesty's government tasked the Security Service – MI5 – both to dismantle jihadist networks and devise a plan to win the hearts and minds of Britain's Muslim minority. Ultimately, the Security Services balked at a difficult job for which they had no experience or clear jurisdiction. We need to do better. Fortunately, unlike our sister democracies across the Atlantic, we have time. We must not squander it. ❖

Falkenrath Testimony *(Continued from Page 13)*

size: these are ongoing operational costs to defend the city.

In the view of the New York Police Department, the threat of terrorism is a global phenomenon that continually presents the possibility of manifesting, at any time, and with catastrophic consequences, in our city. Thus, while the NYPD has a great deal of knowledge of local extremist, radical, and militant individuals and groups, we are equally interested in indicators of terrorist activity elsewhere in the country and around the world. Our reason for this wide view is simple: as terrorists have demonstrated time and again, the efficiency of modern transportation systems – commercial aviation, highways, trains and transit systems, etc. – permits our enemies to conceive, plan, and prepare attacks at far-flung locations, transferring the weapons or operatives to their final target at the last minute. The NYPD does not have the luxury of concerning itself only with our five boroughs, though we wish we did.

Since September 11, 2001, most terrorist plots and attacks perpetrated worldwide have been conceived, planned, and executed by individuals who are part of the local populace and who have only limited, if any, transnational linkages to terrorist organizations abroad. Recent examples of "homegrown" terrorist plots and attacks abound: the recently disrupted terrorist plots in the United Kingdom and Canada, as well as the successful attacks against the London and Madrid subways, to name only four.

New York City is a microcosm of global demographic trends. It contains significant populations from over a dozen countries of terrorist concern. As militant extremism proliferates throughout the world via the Internet, chat rooms, literature, videotapes, sermons, conferences, and traveling militant imams, its effects on foreign as well as domestic Islamic populations appears to be consistent. Despite the success of U.S. overseas efforts in degrading al-Qaeda as an organization, its powerful radical influence on the City's younger generation – especially among its sizeable Muslim community – continues to pose a serious threat from within.

There is no question that many countries – the United Kingdom, for example – face a threat of "homeland" terrorism that is more acute than that faced by the United States. Again, the NYPD takes no comfort in this conclusion. The possibility of a "homegrown" terrorist attack against New York City or any other American city is real and is worsening with time as the radicalization process unfolds.

Recommendations

This is not the setting and, given my current position, I am not the person, to offer a comprehensive assessment of the federal government's efforts to secure the homeland or a comprehensive set of recommendations. The Congress and the Federal Executive Branch have taken countless actions over the last five years that have significantly improved the security of the United States. It is not for me to catalog these achievements. At the request of the Committee, however, I will suggest the following areas in which the federal government could, by doing more or conducting itself differently, combat the threat of terrorism against the homeland more effectively.

Federal Counterterrorism. The implications are obvious: the country is under-investing in the sort of capabilities most needed to combat the most dynamic element in the spectrum of terrorist threats – the "homegrown" element – to the homeland. In combating "homegrown" threats, the burden shifts instead almost entirely to local law enforcement. A "homegrown" threat, like the terrorist plot against the Herald Square subway station disrupted by the NYPD in August 2004, presents few obvious inherent indicators and the few signatures are subtle and embedded within the daily activities of a vast civilian population. Such threats are most likely to be detected by dedicated investigators with both intimate knowledge of the population in question and mastery of human intelligence tradecraft who are backed by the full power and resources of a major law enforcement agency.

Critical Infrastructure Protection. As one of the original architects of the Department of Homeland Security, I say with some sadness that there is no area of the Department's work that disappointments me more than critical infrastructure protection. The problem was rather embarrassingly illustrated by the DHS Inspector General's report that DHS had a database of our nation's vulnerable critical infrastructure, key resources, and national assets that included sites such as Old MacDonald's Petting Zoo in Alabama, a bean festival in Georgia, and the world's largest tin foil ball in Ohio.[1]

The New York Police Department has assessed countless potential terrorist targets in the City, and we monitor the construction or renovation of new potential targets. We have ranked them in terms of the danger they present using defensible analytic criteria. We maintain and carefully guard this list. We maintain a file on each of those potential targets that we assess to present the most serious danger to New York's residents, commuters, and visitors and *(Continued on Page 25)*

[1]http://www.dhs.gov/interweb/assetlibrary/OIG_06-40_Jun06.pdf

Falkenrath Testimony *(Continued from Page 24)*

to New York's economy. And most importantly, we take action to reduce the inherent vulnerability and danger of these top-priority targets.

The precise combination of actions we take depends on the particularity of each potential target. In some cases, we may place or require the emplacement of bollards on the curb. In others, we may temporarily close a street to vehicle traffic, or put in place a vehicle screening check point. In others, we may engage with the owners or real estate developers to convey our sense of the appropriate design basis threat for a new building, and to ensure that these requirements are followed through construction and operation of the building. In other cases, we may deploy a radio car – or perhaps even a harbor launch – with armed officers to an access point to a particularly critical vulnerability. In still others, we might install or require the installation of protective fencing around a particular vulnerability, such as bridge cabling. These measures, and countless other steps like them, constitute critical infrastructure protection. DHS does hardly any of this and provides only diminutive assistance to us as we do it.

In addition to more generous grant support, if the federal government wanted to provide more consequential assistance to the state and local agencies that are actually attempting to protect critical infrastructure, it could do two things.

First, the federal government could recommend a design basis threat and blast performance standard for all major, newly constructed buildings for inclusion in state and local building codes. The Department of State, the Department of Defense, and the General Services Administration currently set such standards for federal facilities. The country as a whole, however, has no such standards though we note that the National Institute of Standards and Technology has recently released a draft set of new construction design standards for comment. The result is that, with few exceptions, major new buildings are being built all across America with almost no regard for their ability to withstand the effects of a curb-side vehicle-borne explosive device. Cities such as New York are forced to grapple with this issue on an ad hoc basis, without any consistent national framework.

Second, the federal government could intervene in the insurance market to promote private-sector insurance against terrorism risk. The percentage of commercial real estate that is insured against terrorism risk has fallen dramatically over the past five years. This development is worrying for a number of reasons, the most important of which is that it reduces an important, market-based incentive for private property owners to build and maintain their facilities to a higher security standard. The disappearance of commercial insurance against terrorism risk has been caused by a number of different factors: most important is that the primary insurers now generally exclude terrorism risk from their standard commercial policies, in some cases not insuring against terrorism risk at all, while in others, selling separate—and quite expensive—terrorism-risk insurance policies, which policyholders generally elect not to take. There is no mandate or expectation that commercial policy writers will insure against terrorism risk.

The market will not address this problem and federal action to date has been inadequate. The Terrorism Risk Insurance Act (TRIA), which was scheduled to sunset in 2005 but extended by Congress to 2007, merely backstopped the reinsurance firms that underwrite primary insurance companies. TRIA's backstopping of the reinsurance market may be necessary but is clearly insufficient for security purposes. To reverse this trend away from terrorism risk insurance across the nation, the federal government should consider adopting, as national policy and law, the mandatory inclusion of terrorism risk in all commercial insurance policies nationwide, without regard to location. ❖

Electric Sector *(Continued from Page 3)*

Participation in exercises: The sector's use of, and participation in, exercises and drills will help reveal weaknesses in procedures and preparation. Complacency and inactivity are serious threats to the sector's ability to respond to national incidents. Active participation in well conceived and conducted drills will be a must in the years ahead.

Collaboration between the public and private sector: The sectors' relationship with our government partners needs to continue to improve. This can be accomplished through full implementation of the Sector Specific Plan (SSP) for the energy sector as part of the National Infrastructure Protection Plan (NIPP).

Education of sector personnel: Our sector will continue to perform well only if our personnel continue to be well trained, informed, and motivated. This is an ongoing task for the sector, and investments in training and education will be required to maintain the expected excellent level of performance. ❖

Legal Insights *(Continued from Page 10)*
training in weapons, explosives and document forgery. On March 29, 2006, he was sentenced to thirty years in prison.

Wesam Al Delaema was also indicted in 2005 on charges of conspiracy of a destructive device during a crime of violence. Al Delaema, a Dutch citizen, allegedly participated in a conspiracy to attack Americans based in Iraq. His were the first criminal charges connected to terrorist activities in Iraq. He faces life in prison.

Additionally, a group of four individuals were indicted on charges of conspiracy to levy war against the U.S. government through terrorism. Three of the four are U.S. citizens and one is a permanent resident. The four individuals were led by an inmate at a California State Prison. The conspiracy began after one of the defendants was released on parole and recruited others at the leader's direction. All four have pleaded not guilty and their trial is set for this fall.

This past year, several individuals have been indicted on terrorism related charges. Jose Padilla, a U.S. citizen held as an enemy combatant for over three years, was indicted in January. He was indicted on charges of conspiracy to murder U.S. nationals, conspiracy to provide material support to terrorists, and providing material support to terrorists. Padilla pleaded not guilty and his trial is set for January 2007.

Three individuals in Cleveland, Ohio were charged with conspiracy to kill or maim people outside the U.S., including U.S. military personnel in Iraq. These were the first charges against U.S. citizens in connection with insurgency in Iraq. The government alleges that three men gathered detailed information on the construction of explosive vests for suicide bombers and the manufacture of improvised explosive devices (IEDs). They also allege that the men attempted to set up training camps inside the U.S. and that they tried to give money, explosives and other materials to extremists in the Middle East. The three men tried to use a car dealership in Ohio and a nonprofit educational program to hide their activities. Their trial date has not been determined.

And finally, Syed Talha Ahsan, a UK citizen, was indicted on charges of conspiracy to support terrorists and conspiracy to kill or injure people abroad. He was a Georgia Institute of Technology student when police arrested him. The government alleges that he and a co-conspirator went to Washington, DC, and took video footage of the U.S. Capitol and the World Bank headquarters and shared their reconnaissance with an alleged terrorist in the UK. The government also claims they were planning an attack against an air base in Atlanta. His trial has not been set yet.

These are just a few examples of individuals charged with terrorism related acts. On June 9, 2005, President Bush said that "federal terrorism investigations have resulted in charges against more than 400 suspects, and more than half of those charged have been convicted." Clearly, law enforcement and prosecutors are fighting terrorism aggressively and forcefully. Due to their hard work, dedication, and perseverance, the United States is safer than it was before September 11, 2001. ❖

Lacombe Interview *(Continued from Page 8)*
talking, planning, and exercises. We see evidence of this happening today with various response plans, strategies, national plans, etc, which are all evidence of the government taking steps to exert leadership.

Is it time to rethink the ISAC framework for information sharing? Are the current ISACs operating effectively, or do the lessons learned over the last ten years suggest that a different approach to information sharing would be more effective?

Lacombe: When we first started proposing ISACs with the PCCIP report, we were proposing them in an environment where none existed. We were looking to find an innovative organizational concept that would provide a means for the sharing of information within the various infrastructures and between government and industry. We looked for a framework that would allow the private sector concerns on sharing information with the government to be accommodated, and to provide channels of communications between the private sector and government. In 1998, when PDD-63 was being drafted, the ISAC appeared to provide this mechanism.

Now, post-9/11, with greatly increased awareness on the part of the nation, the existence of DHS, *(Continued on Page 28)*

Understanding Preparedness *(Continued from Page 2)*
with more than 1,100 partner organizations nationwide we continue to work to educate citizens about the importance of personal preparedness while – at the same time – we are working across government and the private sector to meet our obligations.

The recently thwarted terrorist attack in the U.K. is a good measure of how much better we are doing at coordinating our efforts within the Department, across the federal government, and with our state, local, private sector and international partners. The work involved in the investigation of the plot has been a remarkable example of unity of purpose and effort on many levels and on many fronts. It is exactly what the American people want and what Congress envisioned in creating the Department. Numerous intelligence and law enforcement components worked together seamlessly in a coordinated fashion to address this threat and to take the steps necessary to protect the American public. Late in the day on August 10th, the directions were given to prepare and implement enhanced security measures and to develop contingencies. On the morning of August 11th, when the foiled plot was announced publicly, 10 hours after the national system was energized, security measures were in place and instructions were being delivered to the American people. Initially, some lines to pass through security in many airports across the country were in excess of 2 hours long. At the end of that same day, the average security line was no longer than 38 minutes. This demonstrates that we are on track – we are achieving noteworthy progress in our coordination and communication across government, the private sector and with the American public. People did not simply REACT, they ACTED.

In the wake of the recent five year anniversary of 9/11, and in light of the recently foiled terror plot in the United Kingdom, it is especially important to remember what has brought us – as a Department and as a nation – to our current state. We have to keep this recent history in our thinking and prepare for a wide range of risk that reflects the evolving journey that has brought us to where we are. In the day-to-day grind, critical to our success, also rests the danger that we lose sight of our ultimate goal – a safe and secure America that protects the values we cherish.

Thinking about preparedness as a national responsibility is a benchmark in our nation's history, and is the result of the ebb and flow of multiple ideas. As such it is easy to forget just how pioneering this approach truly is.

Preparedness is the critical link between what we do to prevent, protect and secure our critical infrastructure, and how we respond and recover from disasters. Preparedness is not a federal activity; rather it is a national effort that requires the commitment of each and every individual. Vince Lombardi once said, "Individual commitment to a group effort – that is what makes a team work, a company work, a society work, a civilization work." ❖

Dam Sector *(Continued from Page 6)*
enhanced recovery methods.

Because dam owners are often involved in other sectors, such as energy and water delivery, the DSCC is committed to working with DHS and other federal agencies to get a better understanding of, and agreement on, the nature of the threat to the dam sector, particularly within the context of threats and risks across all 17 CI/KR sectors. That common understanding will allow the sector to make appropriate investments in security programs on a rational and strategic basis, as well as ensure that their strategy for reducing risk across the sector is effective. ❖

Real Estate Sector *(Continued from Page 4)*
was before 9/11. These security-related enhancements include, but are not limited to, investments in additional security personnel, equipment, and other mechanisms designed to monitor and control building access.

As important as these investments are, risk management is not principally about allocating additional resources, but rather, about strategically using existing resources to cost-effectively mitigate risks. Indeed, while it is difficult to put a dollar value on information and experience, these may be our industry's most important assets, in terms of protecting buildings and their occupants against terrorist attacks. The dialogue taking place within our industry about security-related "best practices" — and between our industry and other key commercial sectors — is invaluable. So, too, is the sharing of intelligence between our sector and Federal counterterrorism officials at the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI).

Looking ahead, there are some issues that still require attention. Chief among these is the need to fill some ongoing communication gaps in information sharing. For example, there still needs to be better coordination between local, state and Federal homeland security/intelligence agencies. Also as DHS Secretary Michael Chertoff has said, the nation must do a better job of identifying the most dangerous threats and areas of greatest vulnerability and then allocate federal resources accordingly. In addition, we remain committed to working with policy makers to help the nation prepare for the economic consequences of future terrorist attacks — by making sure businesses and other institutions have access to terrorism insurance coverage and the financial protection it affords against potentially catastrophic losses.

Additionally, the real estate sector should dedicate specific attention to:

- Expanding the effectiveness and relevance of our vital and ongoing information sharing mechanism (the Real Estate ISAC) as well as integrating the information sharing mechanism under development by DHS (e.g., HSIN network) to increase the quality and quantity of inter-governmental as well as public-private sector communications regarding counterterrorism issues.

- Increasing awareness within our industry of the importance of sound emergency preparedness. In each of the last two years, the Real Estate ISAC conducted six-month public service ad campaigns to encourage building owners and managers to play an active role in addressing homeland security issues. In addition, in 2005 the ISAC facilitated the participation of 60+ real estate firms in the national terrorism simulation exercise known as "TOP-OFF 3." That massive biennial drill offered its real estate participants the opportunity to leverage a multi-million-dollar government initiative to exercise their companies' own emergency response plans. We need to continue and improve upon those kinds of exercises. ❖

Lacombe Interview *(Continued from Page 26)*
NCSD, and additional efforts at cooperation across government, the environment has changed. There is a greater exchange of information today than before 9/11. The dynamic changed but the framework is still viable. However, additional investigations into the government's responsibility to support ISACs are very real questions. They still work, but the environment has changed dramatically and the ISACs need to change accordingly.

Pre-9/11, I worried about a lack of attention to the physical side of critical infrastructure protection. From 1997–2001, it was sexier to concentrate on the cyber side of CIP and you didn't see the same level of conversation about the physical side. After 9/11, the appreciation for the physical side, due to the significant impact we witnessed, has brought the focus back to the physical side and the cyber understanding hasn't received quite as much attention over the last few years. While with 9/11 we saw dramatic physical impacts, the impacts of a cyber attack might not have nearly the same loss of life or property. The loss of information translates into economic loss and potentially ruined lives, but it hasn't thus far risen to the tragedy of 9/11 *(Continued on Page 29)*

Lacombe Interview *(Continued from Page 28)*
or Katrina. So there's been a bit of a swing in the amount of attention. But both are very real.

What do you see as the challenges facing CIP in the next ten years?

Lacombe: During the next ten years, one of the challenges we will face as a nation is to take advantage of and implement technology available to enhance CIP—and to exploit technology to win the global war on terrorism. We need technology to share, evaluate, analyze, and use information to support decision making—especially in terms of security planning to incident response, which has incredible potential for the nation; the ability to link together regions, states, municipalities in information sharing and application of analytic tools to it; and, ultimately, our ability to then make better decisions about mitigation and response. During the next ten years, technology advances will provide great opportunities for enhanced protection through sharing of information and between decision making and more effective use of resources both in protection and response. We will see, as we develop these capabilities, if can we achieve the preventative state for which we are looking. ❖

To Keep America Safe / Gov. Warner *(Continued from Page 11)*
federal information. And we need to draw on best practices– for instance, Baltimore's enhanced police Intelligence Unit or the NYPD's SHIELD partnership with the private sector. And since we are asking so much from our police officers, we need a COPS II program to put more officers on the beat.

Third, we need to close glaring gaps in transportation and infrastructure security. We need to deploy systems to screen the contents of every shipping container, screen air cargo for explosives, and set higher standards for security at our chemical plants. We have to get past a knee-jerk anti-regulation view that fails to ask the private sector – which controls 85 percent of our critical infrastructure – to step up and adhere to safer standards and regulations. Many in the private sector would welcome clearer guidance from Washington, because nothing will have a more devastating effect on an industry than a terrorist attack.

Finally, there is a role for every American to play. After 9/11, all Americans would have done anything to step up for our country. But the President didn't ask, and a heavy burden was placed on the backs of our military and first responders. Let's create a truly robust Citizen Corps program. Everyone can play a role, whether it is by being trained to respond to disasters or by finding another way to give back to your community. There are 17,000 more applicants than available spots at Teach for America – we should tap that yearning to serve the common good.

Our response to 9/11 is about more than what we do with our power abroad – it is about what kind of nation we are at home. It is inexcusable that America is more divided today than it was on September 10, 2001. Americans are sick of the politics of Republican versus Democrat, liberal versus conservative, Red versus Blue. Let us use this anniversary to move forward together in a renewed spirit of unity, in this great struggle of our generation. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for The CIP Report, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1