Statement for the Record

George W. Foresman

Under Secretary for Preparedness
United States Department of Homeland Security

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Emergency Communications, Preparedness and Response
Subcommittee on Management, Investigations, and Oversight

"Reforming FEMA: Are We Making Progress?"

February 28, 2007

Good morning Chairmen Cuellar and Carney, Ranking Members Dent and Rogers — Members of the Subcommittee. Thank you for the opportunity to appear before you to discuss the National Protection and Programs Directorate (NPPD).

Strategic Risk Environment

Secretary Chertoff and the Department continue to progress in many areas to manage our full environment of 21st century risk. Our mission is straightforward and guided by five goals:

Goal 1. Protect our Nation from Dangerous People
Goal 2. Protect our Nation from Dangerous Goods
Goal 3. Protect Critical Infrastructure
Goal 4. Build a Nimble, Effective Emergency Response System and a Culture of Preparedness
Goal 5. Strengthen and Unify DHS Operations and Management

Transforming these broad goals into actual results is a complex undertaking. As Congress acknowledged last week with the passage of House Resolution 134, more than 200,000 Department of Homeland Security (DHS) employees are working tirelessly along with their partners across government and the private sector to protect America, its people, and its infrastructure.

The risks that we face come in many forms. Recent attention to the lessons of the August '06 British Air plot and Hurricane Katrina remind us of the wide range of hazards we face. These were headline grabbing events. Equally important but maybe lesser known are situations where vulnerabilities of infrastructure and information technology systems have manifested themselves.

In an interconnected and interdependent global economy, managing risk requires adaptability to a wide range of individual scenarios. These scenarios unite to create a very complex risk environment when it comes to protecting America. The risk environment is dynamic and DHS's approach to managing this risk environment must be equally dynamic.

This approach is focused on the most significant risks, we apply resources in the most practical way possible to prevent, protect against, and respond to manmade and natural hazards. That means making tough-minded assessments, and recognizing that it is simply not possible to eliminate every threat to every individual in every place at every moment. The Department manages risk across a broad spectrum transcending borders and multiple hazards. Discipline is required to assess threats, review vulnerabilities, and weigh consequences; we then have to balance and prioritize our resources against those risks so that we can ensure that our Nation is protected.

Throughout our Nation's history, natural disasters have served as lessons for how to prepare for and respond to the next earthquake, tornado, flood, or hurricane. Decades of experience in dealing with a sheer number of natural disasters globally, has provided sufficient data to understand their risk. By contrast, there have been far fewer terrorist events globally making our comprehension of risk less substantial.

DHS is focused on those possible terrorist events that pose the greatest potential consequences to human life and to the continuity of our society. At the top of that list is the threat of weapons of mass destruction. Weapons of mass destruction are weapons that, if used, could have a devastating effect on this country. Preventing the introduction and use of those weapons has to be the number one focus in the years to come.

We also must continue to guard against infiltration of this country by international terrorists who have the capability and intent to cause damage to the functioning of this country by engaging in multiple deadly attacks on people and our economy. And the illustration of this kind of a scenario is the plot in London that was uncovered last summer. Had it been successful, it would have cost the lives of thousands of people and had the potential to have raised a significant blow against the functioning of our entire system of international trade and travel.

But even as we look at these dangerous threats, we have to be mindful of something else: the potential for home-grown acts of terrorism. We have to recognize that there are individuals who sympathize with terrorist organizations or embrace their ideology, and are prepared to use violence as a means to promote a radical, violent agenda. To minimize this potential emerging threat, we have to work across Federal, State and local jurisdictions to prevent domestic radicalization and terrorism.

Risk is interdependent and interconnected —across communities to nations and must be managed accordingly. For example, a port closure or multiple port closures will not only have an impact on that port area, but also impact manufacturing facilities thousands of miles away that depend on the timely delivery of materials. One of the best examples of this interdependency is petroleum refinery capacity along the Gulf Coast following Hurricane Katrina. The day before Hurricane Katrina, Houston, Texas produced 25 percent of the Nation's petroleum. The day after Hurricane Katrina, with the facilities closed along the Gulf Coast, Houston was forced to produce 47 percent of the nation's petroleum. These examples demonstrate how significant supply chain interdependencies are in managing a full range of risk. So we understand that managing risk requires us to look at a broad continuum across a wide geographical area.

The National Protection and Programs Directorate must be prepared to meet these challenges.

NPPD Mission and Overview

The NPPD will comprise the Office of Infrastructure Protection (IP), the Office of Cyber Security and Communications (CS&C), the United States Visitor and Immigrant Status

Indicator Technology (US-VISIT) program, the Office of Intergovernmental Programs, and the Office of Risk Management and Analysis. This new Directorate will allow the Department to serve as a focal point in enhancing the protection of America by interlacing key programs based on risk.

Currently, there are multiple components within DHS working independently to reduce our comprehensive risk. Three of these components will be located in NPPD — IP, which addresses physical risks; CS&C, which addresses cyber risks; and US-VISIT, which addresses human risks. All three of these offices use the same approach in reducing risk by utilizing data gathering, data analysis, and dissemination of information to operators.

The overarching responsibilities of NPPD are to enhance the protection of national assets, key resources, and people by countering threats whether they are physical, cyber or human. This will be accomplished by advancing the Department's risk-reduction mission and through identification of threats and vulnerabilities to infrastructure and people. In addition, NPPD will synchronize risk-mitigation strategies and Departmental doctrine for protecting America.

The NPPD responsibilities include:

- Promoting an integrated national approach to homeland security protection activities and verifying the approach and strategy via program metrics to assess performance and outcomes against mission goals;
- Protecting people and the Nation's critical infrastructure;
- Ensuring operable and interoperable systems and networks to support emergency communications through a full spectrum of conditions;
- Promoting cyber security
- Standardizing risk management approaches applied across the Department to ensure polices, programs, and resources are driven by a consistent methodology; and
- Enhancing the security of citizens and people traveling to the United States through the use of biometric capabilities.

NPPD will serve the public through these major program activities:

Infrastructure Protection (IP): IP is focused on securing the nation's critical infrastructure through the identification of threats, consequences, and vulnerabilities and through the development of mitigation strategies. Additionally, this activity provides the primary defense against attacks on our nation's critical infrastructure and key resources through robust real-time monitoring and incident response.

Cyber Security and Communications (CS&C): CS&C defends the Nation against virtual or cyber attacks, and incorporates cyber security, promotes operable and interoperable communications for emergency communications. CS&C identifies cyber-based threats, vulnerabilities, and the consequences of successful attacks. It also ensures

the availability and interoperability of information technology (IT) and Communications through the National Communications System (NCS) and the Office of Emergency Communications (OEC).

As part of CS&C, the OEC will work closely with NCS, FEMA, other DHS components, and our Federal, State, local, and tribal partners to improve emergency interoperable communications nationwide. The OEC consolidates the Interoperable Communications Technical Assistance Program and the Integrated Wireless Network program to better integrate the Department's emergency communications planning, preparedness, protection, crisis management, and recovery capabilities across the Nation.

United States Visitor and Immigrant Status Indicator Technology (US-VISIT): Through its deployment of biometric capture and watch list matching capabilities to State Department visa-issuing posts worldwide, U.S. air, land, and sea ports of entry, and U.S. Citizenship and Immigration Services (USCIS) immigration benefit offices within the U.S., US-VISIT supports safe and legitimate travel to the United States. It helps prevent document fraud and identity theft that threaten the integrity of the immigration process and the safety of foreign visitors. US-VISIT also provides key information to law enforcement, border officials, and other decision makers about persons they may encounter in the line of duty, thus protecting their safety and that of U.S. citizens.

Risk Management and Analysis Office: The Risk Management and Analysis Office will lead the Department's efforts to establish a common framework to address the overall management and analysis of homeland security risk. This program will develop a coordinated, collaborative approach to risk management that will allow the Department to leverage and integrate risk expertise across components and external stakeholders.

The Office of Intergovernmental Affairs: Handles communications and coordination activities among State, local, and tribal disciplines across the spectrum of issues confronting all 22 agencies and components of DHS. Daily activities regularly involve contact with, for example, the Coast Guard, Transportation Security Administration, Secret Service, Customs and Border Protection/Border Patrol, USCIS, FEMA – the entire gamut of service providers at DHS – on a host of issues that impact our State and local partners. The Office of Intergovernmental Affairs will liaise with the Secretary, senior DHS leadership and their counterparts across the Nation at the State, local, tribal and territorial levels.

National Protection Planning Office (NPPO): The NPPO will develop doctrine for synchronization of national and regional-level protection plans and actions across Federal, State, local, and private sectors regarding the assessment of both physical and cyber critical infrastructure and key resources. It will develop and coordinate performance metrics to measure progress in reducing the risk to critical infrastructure and key resources. The NPPO will work with other DHS components to synchronize approaches to methodology and develop doctrine for DHS-wide operational planning. This office will perform cross-sector analysis, such as understanding the potential

cascading effects from one sector to another, and recommending approaches to reduce impacts. In addition the NPPO will work across jurisdictions and across borders.

Preparedness Progress to Date

Mr. Chairman I understand the importance of this Subcommittee having the most current, up-to-date information and I would like to highlight for you some important progress made by the Preparedness Directorate as we transition into the NPPD.

Risk Analysis for Grants Process: The Department has made refinements to the data inputs for the risk methodology, taking into account expert judgment, and feedback from Federal, State, and local partners — all with the goal of better understanding risk associated with populations and critical infrastructure.

For example, for critical infrastructure, we looked at nine different variables for each of 260,000 assets in 48 asset classes in FY 2006; and in FY 2007 drew upon a comprehensive national process involving States and sector-specific agencies to arrive at a much more concise list of 2,100 nationally critical assets, streamlining the risk analysis used in the grants determination process.

The National Infrastructure Protection Plan (NIPP): The NIPP is a comprehensive risk management framework that clearly defines critical infrastructure protection roles and responsibilities for all levels of government, private industry, nongovernmental agencies and tribal partners. Seventeen Sector Specific Plans have been completed and are currently being reviewed by the Department as part of the NIPP progress.

Chemical Regulation Authority: DHS was given the authority by Congress to implement risk-based security standards for chemical facilities that present high levels of security risk. This new authority will allow the Department to recognize the significant investments that responsible facilities have made in security, and the ability to ensure that high-risk facilities have adequate safeguards in place.

Buffer Zone Protection Plans: In 2006, 58 percent of identified critical infrastructure had implemented Buffer Zone Protection (BZP) Plans, up significantly from our FY 2005 percentage of 18 percent. The Department worked in collaboration with State, local, and tribal entities by providing training workshops, seminars, technical assistance and a common template to standardize the BZP plan development process.

Cyber Security and Communications (CS&C): DHS' CS&C is aligning to form a cohesive organization to ensure the security, resiliency, and reliability of the Nation's cyber and communications infrastructure in collaboration with multiple public and private sectors, including international partners. Under CS&C the Department has expanded its focus on critical cyber exercising, grants, and management activities.

Interoperability: In December, DHS released the findings of the national baseline survey, which was the first-ever nationwide assessment of interoperability across our country. We engaged more than 22,000 State and local law enforcement, fire response,

and emergency medical service agencies in developing the baseline. The results of the survey show that two-thirds of first responder agencies report using communications interoperability to some degree in their operations. While this is promising, the results also demonstrate that while the necessary technology is largely available, much work needs to be done in the areas of governance, standard operating procedures, training and exercises, and usage. In addition, this baseline survey:

- Determined the capacity for interoperable communications among law enforcement, fire, and EMS agencies across the Nation;
- Established a process and mechanism to facilitate regular measures of communications interoperability;
- Generated data to help emergency response agencies make better-informed decisions about how to most effectively allocate resources for improving communications interoperability; and
- Gathered information to inform future efforts for education, incentives, and planning needed to continue improving interoperability capabilities across the country.

Tactical Interoperable Communication Scorecards: DHS issued scorecards for the 75 largest Urban/Metropolitan Areas. These scorecards measured the ability of Urban/Metropolitan Areas to provide tactical (within one hour) communications capabilities to first responders. This process included the creation of a Tactical Interoperable Communications Plan peer evaluation, full-scale exercise, and after action reports.

Key findings include:

- Policies for interoperable communications are now in place in all 75 urban and metropolitan areas;
- Regular testing and exercises are needed to link disparate systems effectively to allow communications between multi-jurisdictional responders (including State and Federal); and
- Cooperation among first responders in the field is strong, but formalized governance (leadership and strategic planning) across regions has lagged.

The **Nationwide 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.

Collaboration with the Private Sector: DHS has engaged the private sector on a number of preparedness and risk mitigation strategies:

*International Cooperation***:** Partnerships with the World Bank, World Economic Forum, and United Nations on forums focused on public-private partnerships in disaster risk reduction.

DHS also engaged with key allies on cyber security information sharing, as well as other multilateral and international standards organizations such as the Asia Pacific Economic Cooperation, Organization of Economic Cooperation and Development, and International Telecommunication Union, to raise awareness about cyber security and telecommunications standards.

*Ready.gov Business***:** DHS collaborated with the business community on Emergency and Business continuity planning, and on private sector preparedness.

Chief Information Office: Last year the Preparedness Directorate was faced with the Department-wide challenge of bringing all of the IT systems within the Directorate into compliance with Federal Information Security Management Act (FISMA) requirements. The effort to reach FISMA compliance required a full-scale remediation effort to achieve security certification and accreditation for the complete inventory of Preparedness systems. The Preparedness FISMA grade went from being just 8% compliant in June 2006, to 99 percent compliant in October 2006.

This type of progress is significant, but I think we all agree that there is more to do— as we all desire a safer, more secure America. Organizational changes within the Department withstanding, **this mission remains unchanged.**

Change is never easy and one thing that we intuitively know about this environment that we find ourselves in today is it is anything but static. We are building on the significant momentum realized and progress achieved, to promote the ideals of what the Department was established to do – provide for the protection of America and those who live within its borders.

Closing

Mr. Chairman, events such as Hurricane Andrew, the Midwest Floods, the bombings of the World Trade Center and Murrah Federal Building, and more recently September 11th and Hurricane Katrina have granted professionals across the Federal interagency community, as well as at State, and local levels an immense amount of experience in managing response and recovery efforts.

Traditionally, response and recovery involves dealing with defined aspects of an emergency, such as location, size and scale of damage, number of people involved, facilities and infrastructure affected.

Prevention and protection present a much more nebulous and imprecise environment. Therefore, it necessitates an approach to securing our nation that includes the broadest range possible for the full 21st century continuum of risk. NPPD's strategic risk management responsibility encompasses a large spectrum of risk, which includes both economic ramifications and risk to human life. It is not confined to physical borders or corporeal infrastructure.

And at the end of the day – whether our threat comes from our enemies abroad or at home, or from nature, the American people expect that local, State, and Federal government and the private sector are going to cooperate to deal with the challenges that confront them. These early stages of coordinating the expansive spectrum of risk for protecting the Nation will help to catalyze a national transformation for how we prepare America for the risks of the 21st century.

I would like to thank the Subcommittee for its time today and I welcome your perspective on the themes I have articulated.

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

245 Murray Lane, SW
Building 410
Washington, DC 20528
(202) 282-8400

Outline: Testimony includes a discussion of the strategic environment of risk, the National Protection and Programs Directorate (NPPD) Mission and Overview, and a brief overview of accomplishments made by the Preparedness Directorate during the previous year.