Statement for the Record

Stewart Baker
Assistant Secretary for Policy
Department of Homeland Security

Before the

United States House of Representatives Committee on Homeland Security

"The Resilient Homeland: Broadening the Homeland Security Strategy"

May 6, 2008

Chairman Thompson, Ranking Member King, and distinguished members of the Committee, I am pleased to appear before you today to discuss how the Department of Homeland Security (DHS) can build a resilient homeland.

Resilience

Stopping terrorism is a key mission of the Department of Homeland Security. We must make every effort to prevent an attack, but we must do more. As a nation, we must be able to withstand a blow and then bounce back. That's resilience.

Along with planning and preparation, resilience is a part of our approach to homeland security. Resilience is stressed in the Administration's recently-released, second-generation *National Strategy for Homeland Security*, as well as the National Response Framework and the National Incident Management System. Resilience – of our people, our infrastructure, our economy, our entire nation – is an essential element of ensuring the safety and security of the homeland.

Some say that we need to characterize our national efforts to secure the homeland as "resilience," as opposed to "preparedness," or even "homeland security." We should not spend too much time on a purely semantic argument, but there is no doubt that resilience – described by some as our ability to "bend but not break," or the ability to absorb the

impact of a catastrophe without losing the capacity to function – represents an important dimension in our security efforts.

A focus on resilience has value in part because it forces us to acknowledge the limits of government capability. It requires us to admit that some disasters cannot be avoided. It also requires us to acknowledge that, faced with disaster, most of our citizens, businesses, and other institutions will take action to rescue themselves and others. No government can respond as quickly and as creatively as individuals concerned with the well-being of their families, their businesses, and their communities. That is the source of our resilience as a country. While government plays a crucial role as well, perhaps its most important role is creating conditions that allow the creativity and ingenuity of individuals and businesses to flourish.

At the end of the day, building a resilient homeland requires us to trust our citizens. We must inform them – and trust them to inform others. We must equip them with the right tools and technologies – and trust them to use those tools to help themselves and others. I would like to highlight three concrete ways in which the Federal government is creating conditions that foster national resilience: (1) disseminating information that allow individuals to act quickly and wisely; (2) maintaining order; and (3) ensuring the availability of a core infrastructure that individuals will rely on. For the remainder of this testimony, I will offer examples, based on past and present threats, of ways that DHS is creating these three preconditions for a resilient nation.

Information

Ordinary American citizens are our strongest asset in protecting the Nation and ensuring our common security. In order to maximize this potential, however, citizens need information so they can make informed decisions. We can unlock powerful, self-organizing responses to disasters if we can get good information to individuals quickly. New technologies are creating new ways to deliver good information about disasters to

the people who need it most. Our job is to identify these technologies and deploy them where they will do the most good.

When confronted with emergencies or natural disasters, such as the wildfires that raged through San Diego and Los Angeles counties last October or the tornadoes that hit the southern U.S., residents often dial 911 as their first course of action. They are seeking timely and accurate information. There's nothing new about that. But national reverse 911 capability is new, and it is the kind of technology that fosters resilience. Developed by a private company, Reverse 911 uses a combination of database and GIS mapping technologies to deliver outbound warnings to communities and organizations at risk. Reverse 911 played a key role in rescue efforts during the California fires. Automated alert messages were sent to thousands of people simultaneously, warning those who were in the path of rapidly advancing fires. Those citizens then took informed action on their own, providing greater resilience in the face of the threat.

A number of Federal agencies, including DHS, the Department of Transportation, and the Federal Communications Commission, are working on initiatives to make 911 systems more robust, with ability to seamlessly link in advanced technologies with better backup capacity and recovery capabilities. "Next Generation E911" refers to the technologies, such as voice over IP (VOIP); instant messaging, short message service messaging, Wi-Fi, geographic information systems and video, that will allow a broader array of interconnected networks to comprehensively support emergency services - from public access to those services, to the facilitation of those services, to the delivery of the emergency information to dispatchers and first responders.

A resilient response depends not just on individual citizens but on businesses. If disaster strikes a major refinery in the U.S., we could rely on government agencies in Washington to divert supplies from elsewhere to cover the needs of the stricken refinery's customers. Or we could rely on the marketplace to make the adjustments that are needed.

In most cases, the marketplace will be more adaptive and more resilient than a response that depends on government. But, like individuals, businesses are likely to need information that is in the hands of government. To create the conditions for resilience, government needs to communicate reliable, timely, and factual information to businesses. That is the goal of *Ready Business*, part of the Department's *Ready* campaign, a national public service advertising campaign designed to educate and empower Americans to prepare for and respond to emergencies. *Ready Business* provides guidance to small-to-medium size businesses regarding which tools and resources are necessary to plan to stay in business, talk to their employees, and protect their investment.

In preparing for incidents that might affect the flow of trade across our borders, the Department has worked with the private sector through venues like the Commercial Operations Advisory Committee and the Trade Support Network to collect information on what the trade community needs to know to make decisions following an incident that affects the flow of trade. U.S. Customs and Border Protection (CBP) created a web-based communication framework to ensure that we can get pertinent information to stakeholders as soon as it becomes available. It is called the Unified Business Resumption Message and it is available on the CBP website as well as via Remote Subscription Service. While this message template was originally created for the land environment, it has now been tailored to specific modes and there are six live websites for northern and southern border highway and rail, air and maritime. This message is also available through List Serve e-mail based messaging, which sends mode specific messages to the e-mail subscriber.

Sometimes the information people need is not about a fast-moving crisis; sometimes they need information about how to prepare for a particularly dangerous new risk. For instance, there are biological risks, natural or manmade, that fall outside the ordinary experience of the American public. If we expect the public to respond creatively and effectively to these risks, we need to give them the information they need about the risk.

At the same time, biological risks are a classic example of a problem that requires a responsible, resilient response by individuals. Relying entirely on government to address the risk is the opposite of resilience.

Let me explain by looking at a biological risk that is of particular concern – an anthrax attack. If the U.S. suffers an aerosolized anthrax attack, a few hours could make a tremendous difference in the attack's magnitude. Studies indicate that the most prudent response to such an attack is for those who were exposed to take ciprofloxacin or doxycycline.[1],[2], [3] If that is done within 48 hours of exposure, practically everyone will recover. After two days, though, every day of delay means additional casualties. In fact, if medication is delayed by five days, a large majority of those who were exposed will die. So we need to get medicine into our citizens' hands almost immediately after an attack.

What is a resilient response to this problem? Not, I submit, a response that depends entirely on government. Any response that completely relies on the government to distribute medicine to people is fragile. Every organizational failure -- every delay in delivering the medicine, every confusion about who will take which pallets to which distribution centers, every miscommunication about where citizens should go to get their supplies – could result in loss of life. That is the opposite of resilient. Instead, we need to provide citizens with the information they need to respond individually and responsibly to the threat. To the extent possible, we need to encourage citizens to prepare in advance by responsibly maintaining their own supply of cipro or doxy for use in an anthrax emergency.

---

[1] "Public Health Response to an Anthrax Attack: An Evaluation of Vaccination Policy Options;" Prasith Baccam and Michael Boechler, Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science, vol.5, no.1, 2007, pp 26-34.

[2] "Emergency Response to an Anthrax Attack;" Lawrence M. Wein, David L. Craft, and Edward H. Kaplan, Proceedings of the National Academy of Sciences, April 1, 2003.

[3] Systematic Review: A Century of Inhalational Anthrax Cases from 1900 to 2005;" Holty, Bravata, Liu, Olshen, McDonald, Owens, Annals of Internal Medicine, American College of Physicians, February 21, 2006, vol.144, no.4, pp. 270-280.

There are risks in an approach that trusts citizens to treat such a supply responsibly. Overuse of antibiotics has severe public health consequences. But so would an aerosolized anthrax attack. DHS is working with Health and Human Services (HHS) to identify the best options for making sure that public citizens, first responders, and federal employees have cipro/doxy in case of an aerosolized anthrax attack. We are considering all options, including an FDA-approved emergency home medical kit, but that might be several years down the road.

Order

Resilience also depends on our ability to maintain order. If our citizens do not have confidence that they will be safe, that social order will be maintained, then their energies will be concentrated on protecting themselves from a breakdown in social order and not on responding to the disaster itself. The more confident Americans are in government's ability to ensure order, the more resilient our society becomes.

As our *National Strategy for Homeland Security* explains, we are continuing to develop and strengthen comprehensive and effective continuity programs to ensure the preservation of our government under the Constitution and the continuing performance of national essential functions – those government roles that are necessary to lead and sustain the Nation during and following a catastrophic emergency. A national approach to continuity also requires that State, local, and Tribal governments work to ensure that they are able to maintain or rapidly resume effective functioning during and after catastrophic incidents and are able to interact effectively with each other and the Federal Government. Likewise, we strongly encourage the private sector to conduct business continuity planning that recognizes interdependencies and complements governmental efforts – doing so not only helps secure the United States, but also makes good long-term business sense for individual companies. Such integrated and comprehensive planning is essential to protecting and preserving lives and livelihoods and maintaining our robust economy during crises.

In many cases, local and state forces are entirely sufficient to maintain order in the midst of a disaster. But some disasters will strain those resources past the breaking point. To address that problem, as directed by Congress, we are studying the efficacy of establishing specialized law enforcement deployment teams (LEDTs) from neighboring jurisdictions who would be available to assist State, local, and tribal governments in responding to natural disasters and acts of terrorism. We know that the best people to assist State and local law enforcement in restoring and maintaining order are other State and local law enforcement officers. These LEDT teams could be designed to help avoid the confusion that resulted when law enforcement agencies from around the country responded to Hurricane Katrina in an unorganized manner. Without a coordinating mechanism, Louisiana and New Orleans law enforcement teams were forced to deploy out-of-state law enforcement units "on the fly" rather than requesting the specific teams they needed. LEDTs could help provide an organized system that would allow state and local law enforcement to assist each other in quickly resuming normal police services to an area hit by a terrorist attack or natural disaster.

Infrastructure

Finally, the ability of individuals to respond quickly to crises will be greatly enhanced if they can rely on certain core infrastructure.

An old way of thinking about ensuring the ability of key infrastructure to survive terrorist attacks or natural disasters involved investing in redundant and duplicative infrastructure. As noted in our updated homeland security strategy, however, we must instead focus on the resilience of whole systems – an approach that centers on investments that make systems better able to absorb the impact of an event without losing the capacity to function. While this might include the building of redundant assets, resilience is often attained through the dispersal of key functions across multiple service providers, flexible supply chains, and related systems.

No infrastructure is more important to a resilient, self-organizing response than telecommunications and information networks. To build a resilient response, we need to make sure that these networks continue to function in a crisis.

Take the example of a pandemic and dangerous influenza. We know that one is almost certain to strike again, though we don't know when. The pandemic of 1918 had a larger impact on the population of the United States than any other single event in the twentieth century. One of the lessons we learned from that pandemic was the value of social distancing. Those communities with the most disciplined social distancing regimes exhibited the lowest overall mortalities. Social distancing may be even more important in a future pandemic.

Information networks can make social distancing more practical. Telecommuting via the Internet will allow Americans to keep the economy functioning while avoiding crowds and contagion. However, for technology-enabled distancing to work, information technology infrastructure must have the capacity to support a large number of telecommuters. We must also consider how to ensure that the network's bandwidth is not oversubscribed in an emergency.

We must also make sure that the infrastructure can withstand attacks made over our networks. DHS understands that determined and well-resourced cyber adversaries can find their way into most networks. Improving the resilience of private industry and the government to limit the duration and mission impact of successful attacks or cyber incidents is thus a core component of our overall strategy.

Currently, DHS and the Department of Treasury are working with the Financial Services Sector Coordinating Council Subcommittee for Research and Development, along with ChicagoFIRST, an organization dedicated to improving the resilience of financial infrastructure in Chicago, to develop a risk management tool for the finance sector. This

tool is designed to help create a computer simulation of a financial enterprise and its value chains, and how different financial institutions interconnect with others.

Once it is finalized, the tool will allow organizations to create and run multi-party disruption scenarios tailored to their individual business models, using their own proprietary data as well as generic data for the rest of the financial sector. In this way, they can find out specifically how a cyber security event or attack will affect not only their own business, but also learn how the responses of other institutions (including the government) might impact themselves, other in their value chain, and in the sector at large. This improves resilience because it helps ensure all institutions that share a common cyber security incident will make informed response decisions that solve the problem with as little negative impact on the sector as possible.

No single financial company would build such a tool and share it with competitors. However, because of support from DHS, the entire financial sector will be able to improve its resilience by being able to assess and protect itself against emerging cyber security threats.

Conclusion

As stated in the second-generation *Strategy*, "Recognizing that the future is uncertain and that we cannot envision or prepare for every potential threat, we must understand and accept a certain level of risk as a permanent condition." Ensuring our Nation's resilience in the face of all threats is an essential element of our risk mitigation strategy. Our citizens are resourceful and creative in responding to disaster. We need to give them the tools that allow them to use that creativity – good information, social order, and a functioning communications network.