Testimony of Mary Arnold
Vice President, Government Relations
SAP
Before the House Committee on Homeland Security
The Resilient Homeland – Broadening the Homeland Security Strategy
May 6, 2008 – Washington, DC

Introduction

Thank you, Mr. Chairman, Congressman King, and members of the Committee. I am pleased to be here today to speak about the need to broaden U.S. homeland security policy to include homeland resilience – the ability to resume activities after an attack or disaster like 9/11 or Hurricane Katrina.

Today, much of the global supply chain's critical components are in private hands. Certainly, U.S. industry needs to take a proactive role in developing, deploying, and exercising plans that will ensure that a disruption in the supply chain will not result in a crippling blow to their respective businesses. But, government is a critical partner in that process, and for that reason, I want to commend, and thank, the Committee for recognizing the importance of this issue and dedicating the month of May to discussing homeland resilience as a core component of U.S. homeland security policy.

My name is Mary Arnold, and I am Vice President of Government Relations for SAP. SAP is the world's leading provider of business software solutions for government and private enterprise, and the third largest software manufacturer in the world. Because business continuity and supply chain management are critical to our customers, we understand the need for information technology that provides resiliency and redundancy. That is why SAP is the supply chain solution used by a diverse range of private and public sector customers, including over 75% of the Forbes "Global 500" companies, and public sector entities including Clark County, NV, the North Carolina Department of Transportation, the New York Port Authority and the Defense Logistics Agency, to provide them tailored resilient solutions that are flexible, adaptive and responsive. Our understanding is reflected in our over 35 year company heritage of listening to and working with our customers and experts in industries which reflect the entire spectrum of the global economy and public service entities.

Although we cannot predict or prevent every potential disaster, we can identify our vulnerabilities in a variety of scenarios and take steps to reduce them with the right information technology, redundancy solutions, and highly developed continuity-of-operations plans.

Last month, I attended and led a panel at a forum in New York along with 100 other corporate executives entitled: "Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy." In the discussions that took place there, it was clear that achieving resiliency will

require a broad-based and comprehensive solution. Today, however, I am going to focus my comments on the role of information technology.

<u>Perspective from SAP</u>

First, to state an obvious but crucial fact, there are no one-size-fits-all solutions.

Supply chains link thousands of companies in hundreds of industries and dozens of countries. Supply chain solutions must work seamlessly across all of these borders.

There are core elements, such as storage and distribution points, transportation modes, and a supplier-customer relationship endemic to all supply chains. But, there is also diversity in the U.S. and global economy such that what works for one company or industry's supply chain may not reflect the requirements of another. Thus, within every industry, we have seen the need for flexible, adaptive, and resilient solutions. We must ensure that our public policies reflect this diversity and we, as government and the private sector, must work together to ensure that solutions represent the variety of industries, cultures and companies that exist, not only in the United States, but throughout the world.

Second, we need to take an "enterprise" approach to resiliency, or what we might call a "resiliency chain" approach.

By "enterprise" I mean a holistic, all-encompassing perspective. For example, in the energy industry, our vision must go beyond rapid recovery for a single drilling rig, refinery, or pipeline. We need to look at the ENTIRE enterprise from the platform all the way to the gas pump. Similarly, in the defense industry, we speak of "factory to foxhole/flight line/frontline to factory" supply chains. That is, a perspective that reflects consideration of all the events, infrastructure, and players within that supply, or resiliency, chain.

A resiliency chain also needs to have real-time intelligence on alternatives to pieces of the existing value chain, with the existing "value chain" reflecting all the steps and players in which a product is designed, manufactured, marketed, and distributed to customers. For example, if pharmaceutical company "A" is the sole source of a key vaccine, what other pharmaceutical companies have similar manufacturing capabilities, and how could they be rapidly re-purposed in the event of an emergency?

Redundancy is one of the core elements of the resiliency chain. For example, if crucial raw materials normally move by rail, what are the backup plans if our railroads become disabled? If telephone lines go down, what are the backup means of communicating?

Third, we need to consider how to incorporate our global trading partners into our resiliency chain planning.

These partners, too, could be the primary sources of critical inputs, such as energy products; and they, too, could be crippled by natural or man-made disasters. Again, a broad enterprise

perspective and global collaboration will be necessary to ensure our ability to rebound and move on.

Public Private Partnership

What is the best role for government in resiliency chain planning?

The government's role in this context is to be the champion and facilitator of the resiliency chain, balancing the interests of stakeholders, setting broad objectives and strategies, and providing oversight. The private sector can provide the means and the execution. By working together and leveraging the strengths of each, the public and private sectors can accomplish a great deal to improve our national resilience.

Stephen Flynn at the Council on Foreign Relations wrote a fascinating article in the March/April 2008 issue of "Foreign Affairs" in which he stated that sustaining the United States' global leadership and economic competitiveness relied, ultimately, on bolstering the resilience of its society. He went on to describe a need for a sustained commitment to four key factors in order to achieve this level of resilience, which I would like to elaborate on for you today.

First, there is robustness or the ability to keep operating or to stay standing the face of danger. In a public/private partnership, we can work together and make the investment to ensure that our infrastructures, both physically, as well as operationally, are in place to deal with the challenges ahead.

Secondly, we need to focus on resourcefulness, which involves skillfully managing a disaster once it unfolds. For example, Switzerland has developed and fielded a solution which links its country's hospitals, police, fire brigades, executive staff, and the armed forces in its 26 cantons (administrative regions). Active since 2004, the solution underwent its first (and successful) live test in support of the World Economic Forum in 2005.

The third element of resilience is rapid recovery, which is the capacity to get things back to normal as quickly as possible after a disaster. Small towns and large cities across the United States are training their citizens to be auxiliary first responders. This is a perfect opportunity for the public and private sectors to commit resources and collaborate.

Finally, resilience means having the ability to absorb new lessons that can be drawn from a catastrophe. As we have seen in the wake of the September 11th attacks, we have created systems to bolster our critical transportation hubs and homeland security. The private sector is in a prime position to provide resources and play a role in implementing lessons learned.

Identifying Solutions

The private sector can be a great partner and asset to the government in developing solutions to bolster existing resiliency chains. Utilizing already developed, "commercial, off-the-shelf" technology products, that is, products with significant amounts of commercially available IT functionality already built in to them, thus reducing implementation time, cost, and complexity,

we can create solutions that meet the needs and address the diversity of today's public and private sectors. When you look at IT solutions to support resiliency chains, however, keep in mind that you need solutions with the following characteristics:

- The solutions must take in, manage, analyze, and "push" back information to the user based on vast amounts of detailed data;

- These solutions also must integrate information across many large, interconnected enterprises, to become literally a global enterprise;

- These solutions must be based on global standards and reflect an open architecture which can take in data from legacy systems, as well as the latest technology solutions.

- Finally, such solutions must be "technologically agnostic." In other words, they must work with other, open source technologies, such as all types of databases, and cannot be based on one mode of communication, such as a "hard-wired" telephone grid, because that mode of communication may fail in a disaster.

Conclusion

Thank you, Mr. Chairman and members of the Committee. Securing our homeland requires the ability to respond to, and recover quickly from, a catastrophic event, whether natural or man-made. Thus, strengthening the resilience of the nation must be a critical component of our Homeland Security policy.

The U.S. and global economies depend on a just-in-time supply chain that is susceptible to serious disruption that can cripple economic activity. Yet today, the private sector also incorporates resiliency planning, such as keeping track of alternative supply sources and back-up transportation modes, to minimize any disruption to their supply chains.

In order to ensure resiliency and recovery, we must develop public-private partnerships that utilize the resources of both sectors and play to their strengths. We must develop and utilize new technologies that will ensure that we build greater redundancy in our key infrastructure and distribution systems to establish the foundation from which to recover after disaster strikes. Most importantly, we must put our faith in a public and private partnership which, working together, has the knowledge and tools to confront any challenge that we may face.

So again, I commend you, Mr. Chairman, and all members of this Committee for seeking ways to improve our national ability to recover quickly from catastrophic events. We at SAP believe that resiliency must be at the center of U.S. homeland security planning and we stand ready to participate in any and all efforts to achieve this important goal.

That concludes my prepared remarks, and I would be pleased to answer any questions.