WRITTEN TESTIMONY OF

THE HONORABLE THOMAS JARRETT

SECRETARY AND CIO, DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION

and

IMMEDIATE PAST PRESIDENT,

NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION AND INTERNATIONAL SECURITY

OF THE US SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS

JULY 28, 2006

As a representative of the Delaware state government and of the National Association of State Chief Information Officers, I appreciate the opportunity to provide written evidence to the US Senate Subcommittee on Federal Financial Management, Government Information and International Security, in relation to the congressional hearing on Internet disruption and plans for resumption. In particular, I would like to provide comments on the ability for a state government to function in today's world without the Internet or without network availability. A massive Internet disruption and prolonged outage is a topic often discussed at the state level, but a lack of policy and of clarity on the roles that the government and the private sector must each play in reconstitution efforts, are major weaknesses.

My testimony is presented from two perspectives. First, representing the great State of Delaware as Secretary of Delaware's Technology and Information (DTI) agency and state Chief Information Officer (CIO), I would like to describe to you some of the critical services provided by the Delaware state government and how these services would be affected in the event of an Internet disruption; and second, as the immediate past President of the National Association of State Chief Information Officers, or "NASCIO," I would like to present perspectives and examples from my fellow State CIOs regarding this important issue. As background, NASCIO represents state chief information officers and information technology executives and managers from the 50 states, six U.S. territories, and the District of Columbia. In most cases, the state CIO is appointed to his or her position by the governor and have executive-level and statewide responsibility for information technology leadership.

As you are likely aware, the Internet and Internet Protocol (IP) based applications have become critical service channels for government at the federal, state and local levels. The Internet is a significant tool that assists almost every department of state government in day-to-day business operations. It is important to understand that a loss of the Internet would not simply mean that fishing licenses could not be purchased online. It would result in substantial interruptions in critical services to citizens, including our most vulnerable citizens. Whether it's the public Internet or a private Internet state network, the convergence of data, voice, video and wireless has changed the way state government conducts business. For state government, the Internet is now a critical part of the fabric of state service delivery, communications and emergency response. Internet no longer only provides just e-government on a state web portal, but has extended to Voice over IP (VoIP) telephony, IP video conferencing and wireless connectivity. . It is an <u>expectation</u> that state government will use Internet availability to transact services, reach out to citizens and support cross-jurisdictional communications.

It is evident that states have become more reliant on the Internet, however Internet dependency has also trickled down to other sectors of government. Many states have moved services to regional offices and local jurisdictions for convenience and cost savings. Delivery of services to constituents, especially in the human services area, is primarily delivered by local governments on behalf of the state and federal government. A lapse or shutdown in Internet availability would disable a vital state-to-local communications mechanism that supports human services, public safety, revenue collections and many other functions that are state administered and locally delivered or simply local programs delivered locally to citizens via the Internet. In addition, there are specific federally related business areas that would be significantly disrupted

by the loss of Internet access, causing increased economic strain, the least of which would be a loss of electronic remittance systems that utilize secure transmissions through the public Internet to keep commerce moving. In times of disasters and emergency response, the Internet is an important channel for intergovernmental communications among local government, regional governments and the state governments. The public relies on government to issue alerts and warnings – systems which are heavily dependent on the IT infrastructure. This dependence on the Internet that exists within all levels of government, demonstrates a real need for intergovernmental collaboration and cooperation, especially during periods of emergency response.

As the State of Delaware's CIO in charge of all state government information and communications technology, one of my highest priorities is maintaining a robust and reliable state network to serve the citizens of Delaware. In Delaware's emergency management arena, we often say that "every incident is local," and this holds true for the states when it comes to major incidents that could threaten access to the Internet or the state's IT infrastructure. The states cannot and should not depend on the federal government for immediate rescue and response in regard to disaster recovery and business continuity.

In the simplest of terms, at the state level, the impact of a loss of Internet and/or the state's network as the result of a major disruption,, would be catastrophic. The state and the private sector have a symbiotic relationship in terms of operation and infrastructure and if the Internet were to become unavailable, the state could maintain some services internally, but it certainly would not be business as usual. Without an operating Internet or the state's network, the state would be unable to process most type of financial and other key transactions that support the daily business of government.

Further, without access to our network and the internet, public safety and public health would be put at risk. Our State Police would be unable to process background checks, perform license tag lookups, or seamlessly communicate with their local and federal counterparts. Our Department of Corrections would be on full lock-down, our judicial system would be severely impacted and our ability to provide services through our Department of Youth and Families, like Food Stamp processing and distribution, would become virtually non-existent.

Agencies responsible for providing the funds that keep state government operating, especially in the areas of corporations, franchise and gross receipts taxes would be unable to collect revenue. These three sources alone provide 30% of all Delaware state revenue. Our Health and Social Services and Children's departments, along with Corrections and Homeland Security comprise 39% of our expenditures. Again, without the ability to collect taxes and process payments, vital services for our citizens would not continue.

Disaster recovery at the state level requires intense collaboration and cooperation with key private sector vendors, especially those who provide Internet service; wireless and transparent land services; our 800 MHz digital radio system; and the providers of network security such as firewalls and routers.

Delaware, in concert with our primary telecommunications partner, Verizon, has recently applied for telecommunications service priority (TSP) via the U.S. Department of Homeland Security for all of our main trunk circuits as well as 911 centers and 800 numbers. We currently are awaiting notification of approval. Additionally, we are purchasing wireless priority service from Verizon, which also requires federal DHS approval. Delaware's Technology and Information Agency also purchased several satellite phones to facilitate communication between our data centers in the advent that both wireless and wired alternatives are not readily available.

Delaware state government is increasingly focused on disaster recovery and business continuity efforts and my agency has nearly completed our business continuity plan, which has identified over 500 individual processes that are mission critical. Our disaster recovery (DR) drills have increased in frequency from quarterly to nearly monthly and we held our first ever cyber security tabletop exercise last fall, with our second scheduled for this November. Other agencies, such as our division of public health and agriculture departments are also intently involved in contingency planning targeted at specific threats such as the avian flu.

Obviously, Delaware is not alone in its concerns regarding the potential impacts of a major Internet disruption and the challenges of reconstitution. Through NASCIO, a number of states have contributed their perspective and examples of critical services and applications. These examples clearly illustrate the widespread impact in different domains of government activity.

From the Chief Information Technology Officer, State of Kansas:

The Internet is critical not only for e-government, but also for assisting the state's political leadership in managing natural disasters and other crises. A complicating factor is that the population of the state (2.5+ million) is widely dispersed geographically across 82,277 square miles. The Internet is relied upon to be an adjunct command and control mechanism utilizing an application known as Web Emergency Operations Center or simply WebEOC. Using the Internet, various state agencies access a web portal for the exchange of critical information, whether it be tornados or other severe weather, or a terrorist incident. This also serves as a conduit for information to various Federal government agencies, including FEMA. Hence, an Internet connection is crucial to our crisis management scheme whether it be the Kansas Department of Emergency Management or the National Guard.

From the CIO, Minnesota Department Public Health:

The Internet has become a critical service for public health at the federal, state and local levels. The health and safety of Minnesotans has become more and more dependent on the availability of the Internet. While we have made every effort to implement solutions that do not have a single source of failure, we do have several critical functions that would be seriously, if not dangerously, affected by a disruption to the Internet. Below is a partial list of those services.

1. Inability to use phone service, as Minnesota Department Public Health (MDH) has converted to Voice over IP technology. While MDH has retained a few analog phone

lines, phone service would be greatly reduced and our ability to set up Hot Lines for emergency situations would be difficult at best;

2. Inability to communicate vital health information to local public health departments, the news media and partners using email or Websites. MDH would lose the ability to email partners with critical information regarding outbreaks, hazardous events or public health emergencies. This could be especially damaging during a public health emergency, when accurate, timely information is essential;
3. Inability to connect to the CDC for disease and surveillance activities limiting our ability to respond to outbreaks, hazardous events or public health emergencies. (Examples: TB, Influenza, Polio, West Nile, Food Borne Outbreaks, municipal and private well issues)
4. Inability to notify local public health and health care providers about urgent public health threats. The Internet is the primary method of communication about watching for people with symptoms, providing technical details about case situations, assuring messages to providers and the public are consistent.
5. Inability of the Office of Emergency Preparedness to meet the federal requirement to track available hospital beds. This is an Internet-based system and without the Internet, OEP would spend countless hours calling hospitals and hospitals would spend time tracking this issue rather than providing care;
6. Unable to order vaccines through the CDC. States order from the CDC and they in turn distribute the vaccines around the state. This could be life threatening to citizens if there were any kind of an outbreak.

From the CIO, State of Tennessee

An Internet interruption or intentional disruption could impact state government beyond the obvious reduction of the citizen's ability to receive government service via the Internet. Impact would be seen from those state functions which classically use the Internet or an Internet web site as their interface to government systems. Inspectors or auditors working in the field would not be able to provide information or updates which normally come over the Internet. Examples would include those who monitor such things as crop dusters, or health and human service facilities. At the time when communications and the ability to update data and data bases state wide for situational analysis, determination of statewide trends, or impact would be most vital, it would be cut off. While alternative means of update like phone in or physically going to a terminal in a state office which did not rely on the Internet are available, planning for their use and practice of such alternative methods are not well done.

From the CIO, State of Wisconsin:

The largest potential for network outage may no longer be a physical attack on infrastructure, as the Internet protocols were designed to highly resilient, but rather events like bird flu and pandemics. The projected demands on the Internet during a pandemic flu event could overwhelm capacity to due extreme levels of remote access and stress the public Internet to such a degree that most services could no longer be conducted. There was a recent pandemic simulation in Europe that predicts such an outage.

From the Iowa Department of Public Health:

Approximately 2000 private and public healthcare professionals use the statewide immunization registry over the Internet to ensure children get the right shots at the right time and vaccines are distributed when needed. The Women, Infants and Children (WIC) program providing food assistance to families in need requires Internet access to qualify participants and issue checks. The Health Alert Network uses the Internet to provide information to those responding to a health emergency or bioterrorism alert and to help manage incident as they unfold. The last item may be particularly important. A great deal of the planning for homeland security, bioterrorism, response to natural disasters, and the like at the state level relies on the availability of the Internet.

From the CIO, State of Michigan:

Many critical applications pertaining to State Police, Community Health, Transportation, would be impacted negatively. In many instances the reliance upon technology has replaced any procedure or document that would outline a manual solution and therefore if the Internet were down for any extended period of time, these manual processes would need to be developed causing further delays. The following applications/functions would be inoperable for the Michigan Department of Transportation (MDOT):

- **MiPARS** - Michigan Permitting and Routing System - A substantial portion of this system is web-based. This application would likely be mostly or entirely disabled with a loss of Internet services causing delays or complete inability to issue trucking permits and safe routes to the trucking industry. The impact could be a long delay or inability to provide safe commerce distribution throughout Michigan via the trucking industry.

The following applications/functions would be inoperable for the Michigan Department of Education (MDE). The Michigan Department of Information Technology (DIT) hosts over 40 Internet web based applications for Education and CEPI. The primary customers are the 57 intermediate school districts, 550 public school districts and 4500 schools. One example is State Aid Payments to school districts - portions of this system are web based and used to process $11 billion in State Aid payments each year.

From the Iowa Department of Public Health:

Approximately 2000 private and public healthcare professionals use the statewide immunization registry over the Internet to ensure children get the right shots at the right time and vaccines are distributed when needed; 2) the Women, Infants and Children (WIC) program providing food assistance to families in need requires Internet access to qualify participants and issue checks and; 3) the Health Alert Network uses the Internet to provide information to those responding to a health emergency or bioterrorism alert and to help manage incident as they unfold. The last item may be particularly important. A great deal of the planning for homeland security,

bioterrorism, response to natural disasters, and the like at the state level relies on the availability of the Internet.

From the CIO, State of Georgia:

A major concern from Georgia is the recognition that some local government agencies use the internet to connect to state services. A particular concern is local law enforcement access to the FBI's National Crime Information Center (NCIC). Some of the local agencies have migrated their access to the internet with no backup connectivity. The loss of the internet has the potential to put lives at risk by denying officers in the field access to NCIC criminal information.

An extended internet disruption could cause major issues since many agencies have probably leveraged the internet without even knowing it through services offerings. Also, constituent to state communications over the internet is becoming more and more core to supporting our constituents. During Katrina, several agencies within Georgia were using the internet to gather data, disseminate data and otherwise manage the influx of people and supporting their varied needs. The Department of Education was communicating with the other states to share student information in a secure but timely manner. The law enforcement community was sharing information about displaced parolees, etc. The Department of Human Resources was communicating with its peer agencies and the federal government about medical needs.

The many illustrations from my state colleagues represent only the tip of the iceberg of state services and applications that would be severely impacted as a result a major Internet disruption. Yet with all of our individual focus on the provision of services to our citizens and the continuity of government, it is apparent that still is an overwhelming need for increased collaboration within state government, with local governments, between neighboring states and with the federal government. Although states have prepared themselves though redundant provisioning, private backbone networks and business continuity planning, the impact would still be severe.

The lack of a national policy, direction and clarity for Internet resumption will not serve the needs of citizens during a crisis. There is no apparent protocol or process for communication between entities in the advent of an orchestrated large scale denial of service cyber attack or major disaster which would disrupt Internet availability. There needs to be a clear and concise communication system within and throughout all levels of government *and with critical private sector entities such as telecommunication carriers, internet service providers, financial institutions and major it vendors.* NASCIO urges action to determine the appropriate roles and responsibilities of the federal government, state government and the private sector. As the CIO for the State of Delaware and as the Immediate Past President of NASCIO, I appreciate the work of the Subcommittee in addressing this national challenge. NASCIO stands ready to contribute in a meaningful way as needed.