**TESTIMONY OF DAN ROSS**
CHIEF INFORMATION OFFICER, STATE OF MISSOURI
MEMBER OF THE NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS

**BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES**
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

TUESDAY, OCTOBER 23, 2007

---

Chairman Clay, Ranking Member Turner, and distinguished Members of the Subcommittee:

As a representative of the State of Missouri and member of the National Association of State Chief Information Officers (NASCIO), I thank you for inviting me to appear before the U.S. House of Representatives Subcommittee on Information Policy, Census, and National Archives today to offer my perspectives on efforts to secure our nation's Internet infrastructure and to present recovery and response efforts in the event of an Internet disruption. I appreciate the Subcommittee's attention to this important matter and willingness to get input from my viewpoint as the chief information officer (CIO) of the great State of Missouri and from the national perspective as a member of NASCIO.

As background, as the CIO for the State of Missouri I am responsible for the state's Information Technology Services Division, which is the central point for coordinating the information technology policies for the executive branch. The division also promotes economy and efficiency in the use of information technology (IT) and telecommunications for transaction of state business. In addition to my role as the Missouri State CIO, I have been an active member of NASCIO since 2004. NASCIO is the research and advocacy organization representing our priorities and interests. Founded in 1969, NASCIO is a not-for-profit, non-partisan association representing state CIOs and information technology executives from the states, territories, and the District of Columbia. The activities of this association are important because, in most cases, the state CIO is appointed by the Governor and the CIO has executive-level and statewide responsibility for information technology leadership.

As you are undoubtedly aware, the state's critical IT infrastructure, including the Internet, has become an indispensable tool vital to government business, the economy, citizens and national security. It has become the primary method by which the Missouri public receives information

from, or sends information to, government. The public's use of the Internet has replaced much of the traditional walk-in, mail-in, and phone-in structures that had been used throughout our history.

However, this more efficient and effective method of providing public services is not without risk. At the state level, disruption to critical IT applications, systems or a more wide-spread attack on the Internet could hinder, or completely disable state government in day-to-day operations. This could have a severe impact on those among us who are most in need. First responders may not be able to communicate with each other or with citizens during a natural or man-made disaster when time could cost human lives. Critical communications with other levels of government, especially local government jurisdictions, may be disrupted. Vital state-local communications may not be able to relay disease outbreak information in the event of a public health crisis or communicate with the Centers for Disease Control (CDC). 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 purely local programs delivered to citizens via the Internet. The state may not be able to process and deliver important benefits such as family services, food stamp processing and health services to children. Citizens expect government to be at its best when their personal situation may be at its worst.

The regional conditions in my own state illustrate these challenges. A large portion of Eastern Missouri, including the city of St. Louis, sits in close proximity to the New Madrid earthquake fault; so we must remain cognizant of the catastrophic effects that an earthquake could have on the State's telecommunications capabilities. Missouri's capabilities for incident and disaster response depend heavily on the Internet and other wireless connectivity for the exchange of information with mobile response teams.

We must also acknowledge that the Internet was not designed to support the many activities such as public safety and vital health systems that currently rely on it for secure and reliable connectivity. This was emphasized during the past year when major telecommunications outages in Springfield, due to an ice storm, and in St Louis, due to a severe thunder storm, revealed that the State of Missouri is not yet sufficiently prepared to handle major outages to the public voice and Internet network. During these incidents voice communications were nearly impossible, Internet web sites were disabled and cellular communications were severely disrupted during a time when a large number of citizens needed responsive and reliable communication services.

As the nation becomes increasingly Internet and technology dependent, the need to avert a prolonged, large-scale loss or disruption of critical IT infrastructure or the Internet due to a cyber attack, natural disaster, or terrorist incident, becomes as basic as securing our homes, borders and modes of mass transportation. Technology is the common thread among the multiple sectors of the nation's critical infrastructure that provides these sectors' communications and processing capabilities. It allows all of the sectors, from financial institutions, to the energy sector, to the transportation sector, to function reliably and efficiently. However, should an Internet or network disruption take place, it is essential that we have effective and well-coordinated processes in place to ensure successful and rapid restoration of critical IT systems and applications as well as the Internet.

My testimony today will cover such themes, as well as discuss the role of the state CIO in addressing these matters for the enterprise of state government and NASCIO's perspective on the cyber security challenges facing our nation.

**Role of the State CIO in Internet Disruption Prevention and Response**

With an enterprise view of technology policy development, implementation and management, the state CIOs have emerged as key state resources in preventing and developing plans to respond to Internet and network disruptions. While it is difficult to derive a single organizational CIO "model" from the 50 states, protecting the Internet from increasingly virulent cyber threats, maintaining the continuity of critical state IT functions in the event of a disruption or attack, and seeking quick and effective solutions for Internet recovery in the event of a disruption are all intrinsic extensions to the state CIO's role. This is done in coordination and partnership with other state agencies and appropriate federal counterparts.

Missouri established a Cyber Security Office that works closely with our State Homeland Security Office and the U.S. Department of Homeland Security (DHS). We were also one of the founding states in the Multi State-Information Sharing and Analysis Center (MS-ISAC). Two members of my Cyber Security Office are heavily involved with this organization with one co-chairing the Legislative Committee and the other serving on the Operations Committee. Our involvement with the MS-ISAC has greatly facilitated the sharing of information and the tracking of activity that could be harmful to the state.

***Disruption Prevention: Addressing the IT Threat Landscape***

Cyber security is a critical concern of the state CIOs and is consistently a high priority agenda item of my state colleagues. IT security is not only necessary to preserve the states' ability to effectively serve citizens and preserve the privacy of personally sensitive information within the state IT infrastructure, but is a necessary component in securing our nation's Internet infrastructure. Effective IT security is also a foundational component for the technology that enables many homeland security functions.

Fortunately, in the past, Missouri has received State Homeland Security Grant funding from DHS, a portion of which were used to purchase the majority of the technology my organization currently uses to protect our systems from cyber attacks. Unfortunately, we are now struggling to obtain the dollars necessary to maintain the intrusion detection, spam filters and the other technologies originally purchased with the Homeland Security grants.

I know that each of you recognizes that today's IT security domain is in a constant state of evolution as new security threats are created and criminal elements on every continent are seeking to do us harm. Threats to the IT infrastructure are on the rise and hacks, botnets, Trojans, viruses, worms, Denial-of-Service attacks and other suspicious Internet activity continue to compromise the integrity of the Internet and the availability of critical state IT systems and applications. With many IT systems interconnected with each other and to the state

backbone, one incident, in one agency, has the capability to have a widespread impact on state government and beyond.

The sheer pervasiveness of the threats is staggering:

- In Missouri, in FY 07, there were 10,572,000 attacks on the state network and data center – an average of 29,000 per day. Our filters and firewalls block or intercept an average of 327,318 spam emails, 1,701 e-mail viruses and 5,209 web server take-over attempts daily.
- Another state in the Midwestern region has reported 777,606 "high severity" attacks over a three month period from July 2007 through September 2007. Over 80% percent of these "high severity" attacks were brute force attacks against state computer assets. For the same time period, the state reported 2,155,456 "medium severity" attacks, and 4,161,870 "low severity" attacks.
- In Michigan, on an average day, the state blocks 22,059 spam emails; 21, 702 e-mail viruses; 4,239 web defacements; and six remote computer take-over attempts.
- On an average day in Texas state government, there are reports of almost 250 ***successful*** attacks against the state's information resources. A major computer security incident that has significant financial and operational impacts is an annual event for most Texas organizations. Cyber-terrorists, spies, hackers, and thieves are not just targeting Texas computers, though. They are targeting the information that the state's networks store and transmit.

Moreover, the nature of the threats is more worrisome than ever due, in part, to the growing sophistication of attacks. Instead of being targeted by teenage hackers who just want to see which systems they can crack, state IT infrastructure is now being purposefully and maliciously targeted by criminal elements that are increasingly connected with organized crime. They also are increasingly international—attacking state government technology from foreign countries half-way around the globe. These criminals operate for a profit and in an environment where getting apprehended and criminal prosecution are highly unlikely. These trends identified by state security experts are supported by recent findings contained in the CSI (Computer Security Institute) /FBI (Federal Bureau of Investigation) 2007 Security Survey of entities from across the public and private sectors. The study found that financial fraud has overtaken viruses as the greatest source of financial losses and almost one-fifth of survey respondents who had suffered attacks had characterized the attacks as "targeted" to their organization or a subset of organizations.

While many attacks originate from outside state government, there has been rising concern in recent years over attacks and disruptions that originate from within state government. More employees across public and private sectors use technology to carry out their responsibilities and work on-the-go with mobile devices that connect back to workplace IT systems. Major break-downs, disruptions and even purposeful and malicious attacks can arise from within an organization. And, even a major power outage or failure of the electrical grid can impact IT systems on a regional basis.

***IT Infrastructure and Internet Disruption Response: Continuity of Critical Operations and Internet Recovery***

A key component of responding to an Internet and critical IT system disruption is effective planning and coordination. State CIOs are typically responsible for developing and maintaining the statewide communications infrastructure that supports multiple public agencies and institutions, and should be an integral part of any IT planning and coordination process. Increasingly, state CIOs and their IT security personnel forge partnerships with state homeland security, emergency management, law enforcement and public safety officials to plan for the potential of major disruptions and security events. State CIOs are not however, directly responsible for Internet restitution, which is in the hands of private sector carriers providing these communication services under contract to the state.

While state CIOs do play an important part in the security of state IT infrastructure and managing security incidents when they occur, many challenges are associated with this role. For example, some states have greater authority over state agency IT security than others. In states where the CIO may not have explicit authority over the security and resilience of critical IT systems, it may be more difficult for the state CIO to be the primary leader should those systems encounter a severe disruption. Another concern is that funding is necessary to purchase the appropriate security tools, build-in security and resilience into all new IT projects and hire and retain knowledgeable and trained IT security personnel. State IT security competes with other priorities and may suffer if funding is not adequate or sustained over time.

**Recommendations for Improving Upon Current Efforts**

In conclusion Mr. Chairman, I would like to provide the Subcommittee with some recommendations for improving upon efforts that are currently underway. As with most problems, there is no single overarching solution. There are however, a number of important recommendations that should be considered at the federal, state and local level to address Internet and IT infrastructure fortification efforts and to ensure that critical government operations can be quickly restored in the event of a disruption, especially one caused by a cyber attack.

***Internet and IT Infrastructure Fortification***

1. Increased Intergovernmental and Private Sector Coordination: While many at all levels of government are securing their critical IT infrastructure and use of the Internet, forums for the sharing of best practices and the facilitation of inter-governmental security efforts are needed. With more and more IT systems connected to the Internet and connected to each other, we can no longer view security from a narrow, single-organization perspective. Business partners and all levels of government must coordinate to share their best practices and plan for the potential of major, disruptive events.
2. Continued State Involvement in the National Infrastructure Protection Plan (NIPP) and the Cyber Security IT Sector Specific Plan (IT SSP) within it: The NIPP strategy has gone to great lengths to provide instructions on how to mitigate potential attacks that could disrupt government operations in general or homeland security-related, mission-critical systems specifically. In addition, it has helped in setting national preparedness

priorities, identifying responsible parties for specific tasks, and will help to effectively allocate funding and resources to critical infrastructure in need.

3. Identify and Fund Cyber Vulnerabilities: Cyber security is not a tangible asset, and thus, is often not considered a high priority in funding decisions. Federal programmatic funding most often does not include specific provisions for IT security spending to protect federal programs delivered by states. Because of this reality at the state level, there are gaps and inconsistencies in the levels of cyber preparedness. Such gaps make some states and regions more vulnerable to a cyber attack of state systems or Internet disruption. The creation of a funding pool for cyber grants to specifically assist states in achieving their desired IT security posture would be beneficial in raising the overall security of critical IT infrastructure within the state government sector.

***Internet and IT Infrastructure Recovery Planning and Coordination***

1. For planning purposes, a baseline effort is needed that would assist in prioritizing state government services that demand priority attention in the event of a major incident. Make a list of critical state functions that are Internet-dependent. High priority functions that are critical to citizens in need and the most basic governmental functions include:
    - Emergency Response and Communications
    - Communications with First Responders
    - Intergovernmental Coordination during an Emergency
    - Delivery of Human Services (including WIC, food stamps, TANF and other programs intended for those in need)
    - Homeland Security and Public Safety
    - Public Health
    - Communicating with Citizens
    - Law Enforcement, Corrections and Administration of Court Systems

2. Address Internet dependent critical state functions in state continuity of operations and recovery plans
3. Engage with critical private sector entities such as telecommunications carriers, Internet service providers, financial institutions and major IT vendors as well as other levels of government to ensure that physical Internet infrastructure restitution plans have been laid out. A lack of clarity on the roles that the government and the private sector must each play in Internet and critical system restoration is a major weakness. Citizens expect government—whether at the federal, state, or local level—to work with the private sector and with each other when necessary. Internet and IT system restoration councils made up of relevant public and private sector entities should be established to encourage collaboration and increase clarity in the roles that each sector must play.
4. Partake in information sharing initiatives with NASCIO and the MS-ISAC. NASCIO plays an advocacy role with respect to cyber security policy and the role of the state CIOs in protecting critical parts of the nation's critical infrastructure. NASCIO also seeks to ensure that states are integrated with and can provide insight and expertise regarding federal-level cyber security efforts. The MS-ISAC plays a role in coordinating among the states to share threat information and best practices for securing states' IT infrastructure.

**Concluding Remarks**

Technology alone will not solve the security challenges that states face while trying to protect key IT systems and information. Security is highly dependent on policies for information handling coupled with appropriate and reinforced education for all state personnel--not just the information technology staff responsible for handling and protecting the state's information assets. Given the wide variety of security vulnerabilities today, it may only be a matter of time before a state's information systems and assets are compromised. Therefore, it is imperative that an investment in human and technology resources be an ongoing, proactive process; not a reactionary response to a security event. The well-publicized hard costs of security breaches, as well as the soft costs of losing citizen confidence, drive the need for providing sufficient resources for securing the government's information assets and infrastructure.

As the CIO for the State of Missouri and as a representative of NASCIO, I appreciate the work of the Subcommittee in addressing this national challenge. NASCIO is a willing partner in advancing efforts to secure our nation's Internet infrastructure and stands ready to contribute to the Subcommittee in a meaningful way, as needed.