TESTIMONY OF

THE HONORABLE THOMAS JARRETT

SECRETARY AND CIO, DELAWARE DEPARTMENT OF TECHNOLOGY AND INFORMATION

“SECURING CYBERSPACE: EFFORTS TO PROTECT NATIONAL INFORMATION INFRASTRUCTURES CONTINUE TO FACE CHALLENGES

BEFORE THE

SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION AND INTERNATIONAL SECURITY
OF THE SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS

JULY 19, 2005
562 DIRKSEN BUILDING

Thank you for inviting me to appear before you today. I appear in two capacities, first representing the great State of Delaware as Secretary of Delaware's Technology and Information (DTI) agency, and second as the current President of the National Association of State Chief Information Officers, or "NASCIO." NASCIO represents state chief information officers and information resource 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.

First, I would like to say a special thank you to Delaware's Senator Tom Carper and his staff members for suggesting that DTI could contribute a state perspective on the issue of cybersecurity and the importance of protecting states' networks and information. As the State of Delaware's CIO in charge of all state government information and communications technology, one of my highest priorities is cybersecurity. When my fellow CIOs get together for NASCIO meetings, this is the one topic that is always at the top of our discussion list.

The security of Delaware's information technology system is critical to the well-being of our state as a whole, not just the business of the state, but its economy, the provision of federal services to our citizens and homeland security issues such as the protection and support of our first responders. Delaware is unique in that we have centralized the IT functionality across all levels of state government. This centralization helps us to more easily address and focus security efforts than in states where the IT functionality is more fragmented.

In the most simple of terms, keeping those who would wish to do us harm out of our network and systems is the primary challenge of IT security staff in Delaware and across the nation. This requires multiple layers of system protection and constant diligence. Delaware's state network may be small in comparison to some other states, yet we're responsible for over 130,000 users representing all three branches of government including our law enforcement and first responder communities. Additionally, we are responsible for the network welfare of Delaware's K through 12 students in 19 separate school districts, as well as two of our three public higher education institutions.

In 2004 we processed **84 million pieces** of inbound e-mail for state users. Of this, spam accounted for nearly 70% of all incoming mail, viruses accounted for 1.6 million messages and we logged over 100 thousand suspicious activity attempts, sometimes referred to as Trojan Horses. Starting this year, we've deployed new software that permits us to track network events on a daily basis and we estimate that we fend off nearly 3,000 daily attempts at entering our network. As you will see in the documentation that we have attached to the written version of my statement, these numbers are not out of line with what other states are seeing.

As we continue to implement new and better anti-spam and anti-spyware technology, we have seen these numbers drop significantly; yet, last month, (June 2005) our suspicious activity category, —the most dangerous type of all—**spiked from 7,000 attempts in May to 141,000 in June.** This sharp increase is attributable to the latest variant of a "worm" known as "mytopb".

Thankfully, because of our extreme diligence, we have not had a significant intrusion into our state network, however, just last month, one of Delaware's higher education facilities was the victim of an international "phishing" site, and our staff was called upon to make certain that their critical systems were not compromised.

"Keeping those that would wish to do us harm" out of our network requires multiple layers of protection and can make my agency unpopular with some of our users when we require them to remember a strong password, or limit their ability to access certain internet sites. While it is rarely a terrorist in the traditional sense of the word that threatens a state network, we do not focus specifically on who is trying to infiltrate our network. Rather, our goal is to keep all those with bad intentions from ever entering our system, whether they are in-state, in-country or an international friend sending us an e-mail message.

Without lapsing into too many technical terms, we deploy a number of different hardware and software products to protect our network. Some of the terms used have counterparts in the world of physical security—for example, firewalls keep unauthorized computer traffic out of our system, just as a firewall in an apartment building prevents fire from spreading. We use several intrusion detection and protection devices, just like a home security system detects an intruder when a window is opened and protects the residents by sounding an alarm. We even have "black lists" of computer sites that are known to cause problems.

We scan, scan, and scan again, all e-mail coming into the state network. We search for viruses, spam, and other recognized problems. In fact, we have developed working relationships with the FBI and others who perform vulnerability audits and scans for us. The IT arena is an environment where you cannot become complacent at any time. All users of the state network have their outbound connection to the Internet funneled through software programs that block problem websites based on their content along with known phishing sites. All downloads coming into our network are reviewed for viruses and spyware.

During times of heightened security alerts like that resulting from the recent terror incidents in London, we too raise the bar on cybersecurity. While we still practice all of the same system protections, we pay particular attention to the many alerts, notification and security bulletins. We increase our vigilance and our monitoring because we are well aware that a virus that begins in Asia can propagate to the U.S in a matter of a few short hours. In a very short period of time, it is possible for a system that has not been hardened or properly maintained to be completely overrun.

Delaware is the first state to be a part of Microsoft's Security Cooperation Program. This Security Cooperation program provides that Microsoft will issue early notification to us before the anticipated release of security bulletins, alerts and other critical information. We will share metric information with Microsoft regarding attempts into our system. We are also partners in the Multi-State Information Sharing and Analysis Center. During my tenure as CIO, we began an East Coast regional IT Roundtable that includes my peers from New Jersey, Pennsylvania, Maryland, Virginia, and the City of Philadelphia. As "neighbors" we share common borders and common vulnerabilities.

Protecting critical IT infrastructure does not come cheaply. We estimate that we spend $5 million annually, or 15% of my annual budget on security. While we understand the necessity, these are state dollars that could be used for other projects to serve Delaware's citizens.

What does the future hold? Unfortunately I have to state that I believe that threats to cybersecurity will only increase and we will face continual attacks and attempts on multiple fronts. State IT officials must continually adjust how and what gets filtered, blocked or monitored. New threats appear almost daily and they can, in a matter of seconds, render services we've all come to depend upon like email and web browsing, completely unusable. In the worst case scenario, without proper protection and due diligence, an attack could potentially cripple or completely shut down an entire state government.

In the end, we all must understand that all critical infrastructure is the same by its very nature – critical - whether it is a roadway system or a data network. Infrastructure is all about moving people and information, and a state's network infrastructure is equally as important as its highways, electric power grid, or mass transit system.

Now, I will conclude my remarks with a few works about what NASCIO is doing in this area.

NASCIO applauds last Wednesday's announcement by Secretary Chertoff that he will create an assistant secretary for cybersecurity within the reorganized department. NASCIO has supported the calls for such a position and has endorsed past legislative efforts seeking to create the position. The state CIOs have also promoted this position during NASCIO's annual DC fly-ins, where they discuss state and federal IT issues with Congress, including this subcommittee. In fact, the state CIOs have made addressing deficiencies in public-sector cybersecurity the number one item on NASCIO's federal agenda. We believe that the creation of a higher-profile position for cybersecurity within DHS is an important symbolic statement to the nation as a whole. Now, we need to begin work in each of the critical sectors, including ours.

NASCIO has long seen the natural linkage between homeland security and the "state and local sector" CIOs, who oversee information and communications technologies that support the key public service. Section 7(c) of Homeland Security Presidential Directive (HSPD)-7 declares that: "It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could...undermine State and local government capacities to maintain order and to deliver minimum essential public services." Section 15 designates "emergency services"—most of which are delivered by state and local authorities—as being among the nation's "critical infrastructure sectors."

The most disturbing thing that has been discovered by NASCIO's Information Security Committee is the fact that DHS has not included cybersecurity in the state and local planning and preparedness process. In 2003, DHS refined the national program for state-based domestic preparedness (originally developed in 1999) to better meet the realities of the terrorist threat to the United States. Thus, the State Domestic Preparedness Program was reborn as the State Homeland Security Assessment and Strategy (SHSAS) Program. Each State Administrative Agency (SAA)—the primary point of contact between DHS and state preparedness officials—was provided with a 194-page State Handbook, which provides an overview of the entire strategy and assessment process, which is managed by DHS's Office for Domestic Preparedness (ODP).

A review of the handbook revealed that, while chemical, biological, radiological, nuclear, and explosive (CBRNE) WMD threats are addressed in detail, the "cyber" threats to state governments' critical information assets are not addressed at all. Thus, the participation of state CIOs in the DHS grant funding process was very uneven, ranging from high levels of involvement to no involvement at all.

Having provided you with this background, NASCIO comes prepared to offer the committee one substantive step that it can take toward improving intergovernmental cybersecurity. NASCIO has provided committee staff with language that encourages the Secretary to have Office of Domestic Preparedness (ODP) and NASCIO revise the existing strategy and assessment process to include a cybersecurity preparedness plan from each state CIO. That cybersecurity plan would be submitted to ODP by each state as part of the larger SHSAS process. We feel that closing this cybersecurity planning gap in the near term, and especially before the next round of grantmaking gets underway, is the single most important issue facing our sector today.

Finally, NASCIO wants to point out that information systems in general are the only part of the nation's critical infrastructure that is under attack everywhere, all the time—and these attacks are inflicting countless billions of dollars in damage. It is possible that cyber attacks—even those without terroristic intent—could disrupt governments' operations in general or homeland security mission-critical systems specifically. Therefore, it is our duty to secure these systems from all types of threats, regardless of the intent behind them and as soon as possible. As the CIO for the State of Delaware and as the President of NASCIO, I appreciate the work of the Subcommittee in confronting this national challenge.