STATEMENT OF JACQUELYN PATILLO
ACTING CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF TRANSPORTATION

BEFORE THE
SUBCOMMITTEE ON MANAGEMENT, ORGANIZATION, AND PROCUREMENT
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

May 19, 2009

Madam Chairwoman and members of the Subcommittee, thank you for the opportunity to appear today to discuss the state of federal information security, and the Department of Transportation's efforts to comply with the Federal Information Security Management Act of 2002 (FISMA).

I currently serve as the Department's Acting Chief Information Officer (CIO) and Acting Senior Agency Official for Privacy (SAOP).

The Department of Transportation (DOT) Office of the Chief Information Officer (OCIO) has operational responsibility for the Departmental network and communications infrastructure, as well as providing shared services for the Office of the Secretary and for an increasing share of employees in the DOT Operating Administrations as they transition towards use of DOT shared infrastructure services.

The DOT CIO's office also has overall responsibility for the Department's FISMA program and the cyber security posture of DOT networks and information systems. As part of those responsibilities, we must maintain situational awareness of the vulnerabilities and activities on DOT networks and systems, but also seek to mitigate identified vulnerabilities prior to exploitation in order to minimize risks to DOT, Federal, state, local, and to the extent practicable, private systems and data. Where previously we might have limited our focus to just DOT systems and data, in today's world of rapidly evolving threats, interconnected systems, shared services, telework, and cloud computing, vulnerabilities and risks on a given network or system have the potential to impact upon the other networks and systems to which it may interface or be connected.

It is in that context that I come to you today to discuss DOT's FISMA program and progress towards compliance, peer-to-peer (P2P) software, and the recent report from the DOT Office of the Inspector General on FAA web application security.

FISMA Status and Progress

DOT is currently working to make improvements from its 2007 FISMA grade, and the DOT Inspector General's 2008 evaluation of the DOT cyber security program as "not effective." We developed a corrective action plan to address the recommendations made by the Inspector General, instituted regular internal coordination with the DOT Operating Administrations to monitor and drive progress, and reallocated existing personnel and resources to focus on key areas for improvement such as certification and accreditation, verification and validation, and awareness training.

We also have work underway to better define processes, procedures, and metrics for the DOT security program so as to ensure that processes are repeatable, measurable, and sustainable. In doing so, we are seeking to institutionalize these changes within DOT to improve both current and future FISMA performance and compliance, and enhance the resiliency of the program, while retaining sufficient flexibility for evolution of the program as requirements change. We are also actively participating in the White House cyber-security review and expect to implement guidance and recommendations from that effort as they are approved.

Cyber Security Improvements and Institutionalizing Change

On this front, in 2008 the DOT Secretary cemented the role of the DOT Cyber Security Management Center (CSMC) as the DOT enterprise Security Operations Center (SOC) agent for to the U.S. Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security, and established a governing Board of Directors to oversee operations and the strategic direction of the Cyber Security Management Center (CSMC). This action consolidated DOT's cyber security detection, protection, analysis, and response, and cyber security situational awareness in one entity, which streamlined incident handling and improved the detection of unauthorized activities on DOT networks.

Similarly, a pilot implementation of Network Admission Control (NAC) has become an integrated component of the remote access solution for teleworkers and staff working remotely who access the DOT Headquarters network. This Network Admission Control

(NAC) technology permits us to establish policy requirements for computers connecting to the network remotely. This allows DOT to check computers at the periphery before they are allowed access to the internal network. This mechanism checks – among other things – the presence of up to date virus protection, and the existence of peer-to-peer software on the computer requesting access to the DOT network. DOT policy prohibits the use of peer-to-peer software on any DOT asset or computing resources. Computers that fail to meet the requirements are either denied access completely, or are redirected to an isolated web site where patches and updated security software may be downloaded to become compliant.

This capability is also useful in addressing vulnerabilities with employee personal computers used for telework. While we do not scan personal computers used for telework at a detailed level, we can ensure that minimum security requirements are met. This capability was used during the Conficker incident earlier this year to ensure that computers connecting remotely through the DOT secure remote access (SRA) and virtual private network (VPN) systems had active local firewalls installed, and an active antivirus solution. We will be evaluating means to extend this capability to provide coverage at all points of entry into the DOT network.

Building upon Network Admission Control (NAC) and the Cyber Security Management Center (CSMC), we have continued our implementation of the Federal Desktop Core Configuration (FDCC), a configuration standard for Microsoft Windows computers published by the National Institute of Standards and Technology.

Inspector General's Report on ATC Web Application Security

On the subject of the DOT Office of the Inspector General's report on its "Review of Web Application Security and Intrusion Detection in Air Traffic Control Systems", we view the report and its recommendations as instructive not just for the Federal Aviation Administration, but for the other Operating Administrations in DOT and other federal agencies with complex information systems or critical infrastructure responsibilities. The reduction of vulnerabilities in our networks and systems, and mitigation of significant risks is a continuous process that evolves continuously as threat capabilities are ever changing. It requires constant vigilance and skilled individuals using the latest tools to reduce the risk of an attack, and to minimize any implications from an attack, should one occur, whether it comes from inside or outside of our networks.

We take our responsibility for cyber security seriously, and are appreciative of the renewed management attention that the Inspector General's report has drawn to areas where there are fresh opportunities for improvement.

We will be working with the FAA CIO to ensure that the corrective actions to address the issues identified in the report are appropriately implemented. Where there are opportunities to leverage activities, solutions, or lessons learned to the benefit of other DOT programs, we will work with the FAA CIO and the Operating Administration CIOs to deploy solutions across the DOT enterprise in order to minimize risks to all connected systems and stakeholders.

Challenges Remain

As DOT continues to make improvements in cyber security and privacy, we know much remains to be done. Partnerships between the public and private sector to develop more intuitive and proactive mechanisms for dynamic prevention and detection of harmful behavior will facilitate a paradigm shift from a reactive mode to a more dynamic and proactive one.

Summary

In conclusion, I would offer that the Department of Transportation has achieved considerable progress in securing its networks against intrusions and cyber attacks. Nonetheless, there is no reason to celebrate, nor time to rest. Every day we are encountering new threats and new risks, and the capabilities for increasingly sophisticated attacks on critical information technology infrastructure continues to grow. The issues we face are larger than individual departmental CIOs and their staffs. Making progress towards greater network and computer security will be dependent upon effective leadership, both within agencies, and across the Federal government. Staying at least one step ahead of the next cyber attack will require vigilance rooted in a highly skilled IT workforce using the most capable and effective tools available from the private sector. Finally, our networks require the resilience and capabilities to ensure that any intrusions that do occur are promptly detected, quickly and effective dealt with, and the vulnerabilities that enabled the intrusion are swiftly remediated.

Again, I thank you for the opportunity to comment on these important topics, and I look forward to answering any questions that you may have.