TESTIMONY OF DANIEL G. MINTZ
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF TRANSPORATION
BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

July 24, 2007

Mr. Chairman, Ranking Member Davis, and Members of the Committee, thank you for the opportunity to appear today to discuss the important issue of Peer-to-Peer (P2P) file sharing.

My name is Dan Mintz; I have been the Chief Information Officer (CIO) for the Department of Transportation (DOT) since May 1, 2006. My responsibilities include serving as the Senior Agency Official for Privacy (SAOP) and the Secretary's lead for the Department's Identity Theft Task Force. I came to the Government from Sun Microsystems. During my last year at Sun, I chaired a corporate-wide team that studied protection of Federal Government sensitive information within Sun's corporate information systems. The lessons learned from that experience have been of substantial use during my time at the Department of Transportation.

The incident that I will discuss shortly that affected one of my own staff is a classic example of what the Committee has been warning about. Mr. Chairman, as early as May 2003, you said in a statement to this Committee that, "The users of file-sharing programs are predominantly teenagers. We parents and grandparents are too often left struggling to keep up." In my staff member's case, her teenage daughter downloaded LimeWire without informing her parents. LimeWire is a free and readily available

software program that facilitates peer-to-peer file sharing. The result was that a number of Government documents were accessed remotely by a Fox News reporter.

I would like to briefly discuss the Department's approach to security and explain the policies we have put in place relating to P2P software, provide an overview of the P2P incident involving my staff member and, finally, summarize the lessons learned and associated actions we are taking to minimize the likelihood of such incidents occurring in the future.

DOT Policy Efforts as a Result of Federal Information Security Management Act (FISMA) and P2P Software

The Department's Information Assurance Program has made steady progress in recent years to reinforce existing and introduce new security program measures to mitigate the impact of the potential risks posed by P2P applications and other vulnerabilities.

The Department's FISMA score went from a C- in FY05 to a B in FY06 based on these and related steps. However, we continue to be focused on further educating, training, and improving our capabilities in cyber protection particularly as we work to support the Secretary's goal to increase the Department's telework capabilities and capacities.

The Office of Management and Budget's (OMB) inclusion of a question in the annual FISMA reporting requirements regarding department and agency incorporation of policies and training with respect to P2P first began in the FY2005 FISMA reporting cycle.

On May 11, 2006, I issued DOT Information Technology and Information Assurance Policy Number 2006-17: Peer-to-Peer (P2P) Software Policy. This policy

provided updated procedures and assigned responsibilities for ensuring protection against security incidents related to Peer-to-Peer (P2P) software applications. Complementing the issuance of this policy, the Department's annual security awareness training program was updated to include information discussing the vulnerabilities associated with the use of P2P file sharing software as part of the annual training material.

I would like to emphasize two key provisions of our current P2P policy:

- DOT users are not authorized to install or use software applications on DOT computers and networks unless expressly authorized in writing by my office. Written authorization must be provided prior to installation of P2P software, if the need has been determined to allow the use of P2P.

- All DOT networks are monitored to identify the use of P2P software. If the use of P2P software is identified and if no written authorization exists for the use of the software, it will be removed immediately and appropriate disciplinary action should be considered.

As further background on our policy approach, the Department issued its first policy and guidelines addressing P2P file sharing applications on November 7, 2003, two years before this issue was included in the annual FISMA reporting requirements. In September, 2004, OMB issued guidelines for the use of file sharing technology. The Department's initial policies and later updates responded to those guidelines including: creating policies, training, and implementing security controls.

DOT Efforts to Manage Peer-to-Peer (P2P) Software Usage

P2P software poses a significant risk to Departmental systems and networks as well as home computers. Others will focus on the details of how such software works and its potential impact, therefore, I will not deal with those topics here.

However, I do want to point out that peer-to-peer networks can be difficult to detect by intrusion detection systems (IDS), and most firewalls do not stop peer-to-peer traffic, because the peer node on the inside of the firewall initiates a connection to other peers. Once the internal node connects to an external network, any other peer node in the world will have access to the user's desktop. Since the user desktop is a portal to critical DOT assets and resources, the internal peer node could provide any user in the world access to DOT systems.

Moreover, the current method of detecting P2P is through the installed base of Intrusion Detection Systems, which is less than perfect. The detection of P2P traffic using network based IDS's generates numerous false positive alerts, because the detection approach is to look at specific ports on the network for P2P activity. Often legitimate software will utilize the same ports that P2P software is traditionally seen on, creating a false positive alert.

Security incidents at the Department are recorded and managed by the Transportation Cyber Incident Response Center (TCIRC). The TCIRC provides the Department's IT infrastructure cyber-situational awareness. It is also the sole organization that coordinates and correlates all cyber-events with the Department of Homeland Security. The TCIRC is used by my office for major portions of FISMA

compliance reviews and maintains a continuous monitoring capability to address the cyber-health and welfare of the DOT information technology (IT) systems and network.

The TCIRC treats detected P2P activity just as it does any other cyber security issue. When P2P activity is identified, the TCIRC staff use several tools in an attempt to identify the offending system. After identifying the offending system, the TCIRC works with security staff to identify the physical location of the system and take action to remove the system from the network and remove the P2P software from the system. It is current TCIRC policy that all P2P activity identified on any DOT system be reported to the United States Computer Emergency Readiness Team (US-CERT). US-CERT is a partnership between the Department of Homeland Security and other public and private sectors established in 2003 to help protect the nation's Internet infrastructure.

DOT cannot restrict the use of peer-to-peer software on personal laptop or desktop computers. However, DOT policy prohibits employees and contract staff from using, processing, storing, or accessing DOT information or systems if P2P software is installed or suspected of being installed on an employee's personal computer.

Overall, DOT maintains a constant vigilance on any cyber event that could cause harm to our networks. P2P detection is one of those events.

DOT Implementation of OMB Policies

There are two policies that OMB has issued that DOT uses to provide guidance regarding protecting and responding to breaches of personally identifiable information, M-06-16, issued June 2006, and M-07-16 issued May 2007. As part of on-going security

and privacy efforts, DOT has worked to implement the requirements of OMB M-06-16 and OMB M-07-16. Specifically, we have:

- Established a departmental policy for the protection of personally identifiable information (PII) and sensitive personally identifiable information (SPII), including core requirements for encryption of SPII at rest, in transit and in store.
- Created the procedures described above for handling incidents involving the suspected or confirmed loss of personal information.
- Surveyed all IT system owners on the administrative, technical, and physical safeguards in place to protect personal information. The 2007 system survey is currently underway as part of our broad review of PII holdings.
- Deployed a best-in-class FIPS 140-2 compatible encryption solution on all Department laptops.
- Established a senior official team to respond to large-scale breaches.
- Moved to reduce the unnecessary collection and use of Social Security Numbers in programs and systems, and to mask those numbers whenever possible, if their use or collection is necessary.
- Initiated the revision of policies and procedures to reflect new requirements aimed at preventing and responding to breaches involving PII.
- Selected a solution for providing enhanced security training to all employees and contractors involved in the handling of PII and launched annual privacy awareness training.

- Used broadcast messages and other mechanisms to remind employees and contractors of new security and privacy issues and to remind them of their responsibilities to safeguard personal information.

While we have made important strides at DOT in the area of privacy and security protection, we are reminded by incidents, such as the P2P event, that we must remain vigilant about keeping employees informed of new threats as well as instituting new policies, procedures, technologies and tools to protect the data that resides on our networks.

DOT P2P Incident

My staff member, like many employees at the Department of Transportation, performs work at home. She does so because she has received approval to telework and also because there are times when she needs to perform work in the evenings or on weekends.

In about March of this year, her teenage daughter downloaded LimeWire—most likely to share music or similar files—without at the time informing her parents. In early May, a news reporter for Fox News accessed my employee's personal computer and several Government documents.

On May 4th, the reporter contacted my staff member by email, and informed her that he had accessed her personal computer and a number of Government-related documents. She contacted her manager, who reports to me, and we put her in touch with the DOT Office of the Inspector General (DOT OIG).

As part of their investigation, the DOT OIG performed a forensics analysis on the thousands of files on her computer, and identified approximately 93 DOT-related

documents and approximately 260 National Archives-related documents, where she worked before coming to DOT in January 2007. Not all of those documents were publicly accessible at the time. The OIG has found that 30 of the approximately 93 DOT-related documents were publicly accessible at the time via LimeWire or other P2P software by virtue of residing in a "shared folder," while 36 of the approximately 260 National Archives-related documents were in a shared folder and thus publicly accessible. None of the DOT documents identified contained sensitive personally identifiable information (SPII) about any other employee other than my staff member herself.

The DOT OIG has briefed me on their investigation and is completing a final report. Assuming nothing unexpected turns up as the DOT OIG concludes its review, we are planning to close the incident without a formal personnel action. The person in question has been an excellent and valued employee at the Department; she made a mistake. While we do not believe that disciplinary or other personnel action involving our employee is warranted, the CIO Office has assigned her a number of tasks directly related to reviewing current policies on home computer use and potential problems associated with peer-to-peer networking and providing recommendations for strengthening these policies. In addition, the employee will assist in developing appropriate training for agency employees concerning the proper handing of SPII.

Lessons Learned

In many ways, this incident and the nature of the people involved illustrate the challenges we face and the need for continuing due diligence on all of our parts. An incident occurred involving an employee who has consistently performed well and

approached her work in a professional manner, at a Department that has been improving its overall security, with policies in place that cover these issues in general and P2P specifically, and a training program that emphasizes these policies.

Yet, in this case, none of these were sufficient to prevent access to Government documents when a young family member downloaded software that she did not realize would be capable of exposing these documents to anyone else using the same or compatible software.

In response to this, the Department will be taking a number of initiatives that we strongly believe will both make the security infrastructure more robust and more aggressively make these issues more visible to DOT staff. The first three are broad initiatives dealing with the overall security organization and policy, the remainder deal with specifics relating to P2P.

First, we are performing an in-depth review of the security architecture that has now been integrated at the Department's new headquarters building at the Southeast Federal Center (SEFC). Historically, the Department has had individually managed networks run by each Departmental agency. Administrative rights policies, hardware and software configurations, and network implementations were often inconsistent and inconsistently applied. The Department has committed to follow the recently promulgated standards for Microsoft Operating Systems put together by the Air Force, Microsoft, and OMB, and will shortly be putting in place rules and a transition strategy to simplify the overall network. This, plus the installation of centrally managed network security software, will make us better able to monitor the usage of permitted software and detect the usage of non-approved P2P software.

Second, the Federal Aviation Administration and the rest of the Department are moving to merge the two incident centers that each currently separately manages to create a single, integrated approach for Department-wide monitoring. This will make more efficient use of Departmental resources and establish an additional step in increasing the security posture to monitor these kinds of incidents.

Third, we have asked the DOT OIG to work with us in reviewing the totality of the policies that currently exist and help us determine which ones are effective and where there are gaps in the policy that need to be filled.

Fourth, we are expanding our emphasis to move employees to laptops from their more traditional desktop configurations. In this fashion, we will increase the percentage of employees who have Government owned equipment at home. And by policy and practice, all laptops are encrypted with FIPS 140-2 compatible Department of Transportation provided software. Agencies of the Department, such as the Federal Railroad Administration and the Pipeline and Hazardous Materials Safety Administration have already moved many of their employees to laptops. We will work with the DOT Telework Committee to identify those employees who have already been approved for telework plus those that would likely be key participants in any Continuity of Operations (COOP) event and be the first candidates to move to laptops when we perform a desktop refresh.

Fifth, we will be implementing a number of steps to improve the messaging regarding P2P to new employees and in particular those who will be involved with telework.

- We will prepare examples of home desktop configuration guides that teleworkers can use to set-up their home PC. While these will only be guidelines, it is clear that home workers are looking for advice on how to secure their systems. As a supplement to our current annual security training for all DOT employees, we will be creating telework specific training which will include information on threats facing home PCs.
- Finally, we will ask all employees upon their departure from the Department to verify that all Departmental information has been removed from the employee's home computer.

Summary

In conclusion, it is my observation and experience at DOT that while progress has been made in managing threats stemming from P2P file sharing, we must remain vigilant about educating our employees about these dangers and developing and implementing policies, procedures and technologies aimed at safeguarding our networks and sensitive data. At the same time, we must balance this vigilance against the many positive, legitimate uses of P2P for improving government efficiency and productivity.

Finally, we need to recognize that regardless of the policies that we put in place and how we make those policies available to our employees, the continual audit of their effectiveness and continual reinforcement of our policy goals will in large part determine their effectiveness.

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