

TESTIMONY OF  
THOMAS N. PYKE, JR.  
CHIEF INFORMATION OFFICER  
U.S. DEPARTMENT OF COMMERCE  
BEFORE THE  
COMMITTEE ON GOVERNMENT REFORM  
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,  
INTERGOVERNMENTAL RELATIONS AND THE CENSUS  
UNITED STATES HOUSE OF REPRESENTATIVES

APRIL 8, 2003

Good morning, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer of the Department of Commerce. I am pleased to be here this morning to share with the Subcommittee a summary of the actions the Department of Commerce has taken over the last two years to strengthen our cyber security, or information security, posture.

The Department's actions to improve its management of information security started at the top. Secretary Don Evans directed all Commerce agency heads to focus their attention on establishing information technology (IT) security as a priority in June 2001. He directed that they allocate necessary resources to ensure that the Department's data and information systems are adequately protected against risks resulting from misuse or unauthorized access. This important action ensures accountability for IT security by all of the Department's senior managers, and both the Secretary and Deputy Secretary Sam Bodman have emphasized this personal responsibility of Commerce agency heads as they have communicated with them about the importance of IT security during the last two years.

The Secretary also instituted a Department-wide IT restructuring plan that empowered the Department's CIOs by providing them with the necessary authority to manage IT security as well as IT planning and operations and IT capital investment review. As the Department CIO, I issue IT security policy and provide IT security guidance to the Commerce agency heads and to their CIOs. I participate in the annual review of the performance of each of the Commerce agency CIOs, which bolsters the authority I have to ensure effective management of the Department's \$1.5 billion annual expenditure on information technology, including the protection of our IT resources through a Department-wide IT Security Program.

We have issued in January 2003, a comprehensive, Department-wide IT Security policy, as well as minimum standards for management, operational, and technical controls and other key aspects of implementing this policy. We also issued a password management policy, in June 2002, and a Remote Access Security Policy, in December 2002. Policy implementation guides have been issued that address corrective action planning to identify and correct security weaknesses, documentation of security and privacy in the IT capital asset planning process, and maintaining complete inventories of the security status of all IT systems.

The Department instituted a compliance monitoring process in 2002, through which we determine Commerce agency compliance with Department IT security policies, standards, and guidance. This process includes tests of all management, operational, and technical controls, including tests of systems and networks, to ensure that they are

adequately protected against unauthorized access. We have also established an IT security training program, through which every Commerce employee and contractor employee has received IT security awareness training, and is receiving updated training every year. Specialized training for IT security personnel, managers, and system administrators is also being provided.

The Department has established a computer incident response capability that supports actions to protect systems and data when incidents occur, and facilitates proper reporting of incidents. A Department-wide IT security alert capability has also been established, that ensures 24 hours a day, 7 days a week transmittal of IT security alerts throughout the Department and activation of Commerce agency emergency mobilization plans, as appropriate.

Especially since the Commerce Department has been “coming from behind” as it has implemented this comprehensive IT security program, numerous corrective actions have been identified that need special attention to correct identified weaknesses. A Department-wide database of needed corrective actions has been created and is being maintained. It includes every IT security action resulting from GAO and Commerce Office of Inspector General audits, as well as actions resulting from Department IT security compliance reviews and Commerce agency self-assessments. We expect to complete by this September all of the corrective actions that were open at the beginning of FY 2003. Over 74% of these actions are already completed. We also expect to have

completed by the end of FY 2003 all but two of the over 200 new needed corrective actions that have been identified during FY 2003.

The top level measure we use to manage IT security across the Department is what we call IT security program “maturity.” By the end of FY 2003, we expect that every Commerce agency will be operating at least at a Level 3 maturity, which requires that all IT systems have implemented policies and procedures. We have identified our national critical and mission critical IT assets and the IT system components of those assets, and we expect to have certification and accreditation for full operation of these systems completed by the end of FY 2003. This represents a very important step toward a greatly strengthened Department-wide IT security program.

I would like to call to your attention a resource that has been especially helpful as we have strengthened the Department’s IT security program. This resource is our very own Computer Security Division within the Department’s National Institute of Standards and Technology. The standards and guidelines and related products issued by the Computer Security Division are intended for use throughout the Federal Government, and I am proud to say that the Department itself is benefiting significantly from use of these products.

Thank you for this opportunity to tell you about what we have done in the Commerce Department to improve our information security posture. We have come a long way during the last two years, and we are working hard to complete the next steps that are

essential to provide adequate protection of our data and systems. We understand, however, that IT security is a never-ending process, and we are committed to maintaining a high level of vigilance to ensure that the Department is able to carry out its mission without disruption caused by cyber threats. I would be pleased to respond to any questions you may have.