STATEMENT OF DR. DANIEL J. MEHAN, ASSISTANT ADMINISTRATOR FOR INFORMATION SERVICES AND CHIEF INFORMATION OFFICER, FEDERAL AVIATION ADMINISTRATION, BEFORE THE SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS OF THE HOUSE COMMITTEE ON GOVERNMENT REFORM, ON INFORMATION SECURITY, JUNE 2, 2004

Good afternoon Chairman Putnam, Representative Miller, Members of the Subcommittee:

It is my pleasure to appear before you today to provide a perspective on the challenges of securing information systems in a federal civilian agency and to share with you the model the Federal Aviation Administration (FAA) has developed to address these challenges over the next several years. I would like to commend the Subcommittee for holding this hearing in order to highlight the important work that agencies must do to protect vital government systems. I would also like to emphasize that the FAA works collaboratively with the Department of Transportation (DOT) in all aspects of our Information Technology (IT) Security Program, and to acknowledge my colleague Lisa Schlosser, the DOT Associate CIO for Information Technology Security, who is with me at this hearing. In all of our activities, DOT and FAA work closely with other government initiatives. For example, we share incident information with the Department of Homeland Security's U.S. Computer Emergency Readiness Team (CERT), and we have also worked with the National Science Foundation, the Air Force Research Lab and other government cyber security experts on a variety of research topics.

The FAA maintains, operates, and regulates the largest and most complex aviation system in the world. Effective management of this vast and complex web of information about aircraft, weather, runway conditions, maintenance facilities,

navigational aids, and a myriad of other elements is paramount to accomplishing our mission. This emphasis on information management brings with it a need to ensure that data is neither corrupted nor disrupted as it is shared across today's interconnected world. To secure its cyber infrastructure, the FAA has developed and is implementing an "*android"* model for cyber defense (see attached pictorial diagram) that emulates one of the most resilient systems in the world—the human body. This "holistic" view enables the agency to address both short-term and long-term cyber security objectives within the context of a unified framework.

There are six principal elements of the android cyber defense; and they are analogous to six facets of the human body's defense. The three on the left side of the *android*--architecture simplification, element hardening, and boundary protection—are the ones that have received the most attention historically, and I would like to address them first.

- Architecture simplification is analogous to nutrition and exercise. It is designed to ensure that the cyber infrastructure is in "good shape" to resist an attack. In this area, we are working on the development of a technical reference model, common access architecture, and desktop standards that will become the roadmap for effective information technology applications and services in the future. We are also ensuring that the number of systems in our inventory declines over time as we establish more streamlined information technology architecture.
- Element Hardening is analogous to protecting major organs, such as the heart and lungs. This element focuses specifically on ***vulnerability management*** since it is about discovering vulnerabilities, setting priorities to conduct remediation, and

applying appropriate resources for our critical systems. The FAA will complete security certification and authorization packages (SCAPs) on more than 95 percent of the systems in its inventory by the end of this month. Each SCAP has a plan of action and milestones that identify the most effective strategy to remediate vulnerabilities. In addition, more then 1600 FAA servers are scanned on a regular basis in order to identify and reduce the number of vulnerabilities per server. Both the SCAP completion targets and the vulnerability reduction targets are reviewed with the Department's Office of the CIO and are included as key metrics in the FAA's overall management plan, known as our *Flight Plan.* Our *Flight Plan,* which is reviewed monthly with Administrator Blakey, links the agency's activities through 2008 to our budget requests. It aligns all of our business plans, including information services, to ensure accountability at all levels.

With respect to patch management, the FAA has established policy and is currently using patch management tools to deliver software patches on our systems. In a broader context, we are working with the Department's Office of the CIO to complete the requirements for a DOT-wide patch management tool set. Such a tool set will allow for an enterprise-wide license and standardized approach to patch management for all DOT operating administrations, a significant contributor to securing the enterprise.

- Boundary protection is analogous to skin and membrane; it is the first line of defense against invaders. The FAA has significantly improved its boundary defense through three initiatives: first, reducing the number of authorized internet access points; second, implementing a new e-mail system and reducing the number of mailboxes

from 855 down to 12; and third, by beginning to deploy the FAA Telecommunications Infrastructure, a communications network that is fundamentally designed to provide a higher degree of computer security.

We believe there are tangible benefits being gained from our focus on these three left side elements of the *android*, most notably demonstrated by the fact that the agency and the Department have fared well in the recent cyber storms of Sasser, Blaster, and Nimda. That said, there is *much more to do*.

The FAA is on a path to modernize its air traffic systems and to use more commercial off-the-shelf products. With this significant emphasis on implementing air traffic control enhancements, the agency will also improve its layered protection scheme by augmenting the three elements on the right side of the *android* model: orderly quarantine, systemic monitoring, and informed recovery. These critical elements describe the "other side" of our cyber security concept:

- Orderly quarantine is analogous to the human body's immune system. We need a cyber immune system that can find, analyze, and cure previously unknown viruses faster than the viruses themselves can spread. Human intervention must be eliminated for portions of the defense because of the necessity to react very quickly. Increased research will be required in the coming years to develop practical defense capabilities in this challenging area. In addition, it will take considerable policy discussion, operational analysis, and system testing before those charged with protecting the an agency's network, the FAA's for example, will "turn over" the

quarantining of significant portions of it to an automated security system. So an enormous amount of research and development is required in this area in both the public and private sector, and it is an area where people, process and technology need to be blended.

- Systemic monitoring is analogous to monitoring the vital signs of the body on a continuous basis. The FAA wants to implement IT infrastructure and systems that can detect failures in real or near-real time and protect and heal themselves. This capability requires the system to know its environment and act accordingly. Self-awareness and autonomic capabilities are still largely embryonic. One challenge in these operations is that input from a large number of network sensors often exceeds millions of packets per day, potentially triggering thousands of alarms. The FAA has begun incorporating into its Computer Security Incident Response Center (CSIRC) into a data fusion center, using the next generation of tools to conduct data aggregation, data reduction, event correlation, and to detect anomalous behavior. Vendors are beginning to offer enterprise management consoles that attempt to provide "self-healing," but this is an area that needs to become much more mature in the near future. This model is also being piloted with DOT and the Department of Homeland Security to assist in creating near-real time information sharing that can ultimately be leveraged to protect the entire national infrastructure from the cyber threat.
- Informed recovery is analogous to medical regimens such as administering antibiotics and undergoing surgery. Informed recovery in complex information systems is the set of actions that occur after there has been a cyber security incident. For the FAA,

these actions will include advisories from our CSIRC and the Department's Transportation Cyber Incident Response Center (TCIRC), established procedures to be followed during an alert, and orderly backup and recovery mechanisms. Since a key requirement is to shrink response time, one of the near term goals is to converge vulnerability scanners, trouble-ticketing programs, and patch management software. The desired outcome is to automate more of the process from scanning to notification to remediation. The private sector can advance this initiative significantly by designing systems that export system message logs to an external bus in a standardized format, so that the information could be used in real time with the other data sources.

To conclude, Mr. Chairman, the FAA, with the entire Department of Transportation, is complying fully with the Federal Information Security Management Act (FISMA) and has fared well using its multi-layered defense approach in the face of recent viruses and worms. That said, cyber defense over the balance of this decade needs to rely on the total *android* and requires effort in areas where it is frankly more difficult to set up scorecards and audits. For the FAA, we will meet this challenge using a three pronged approach:

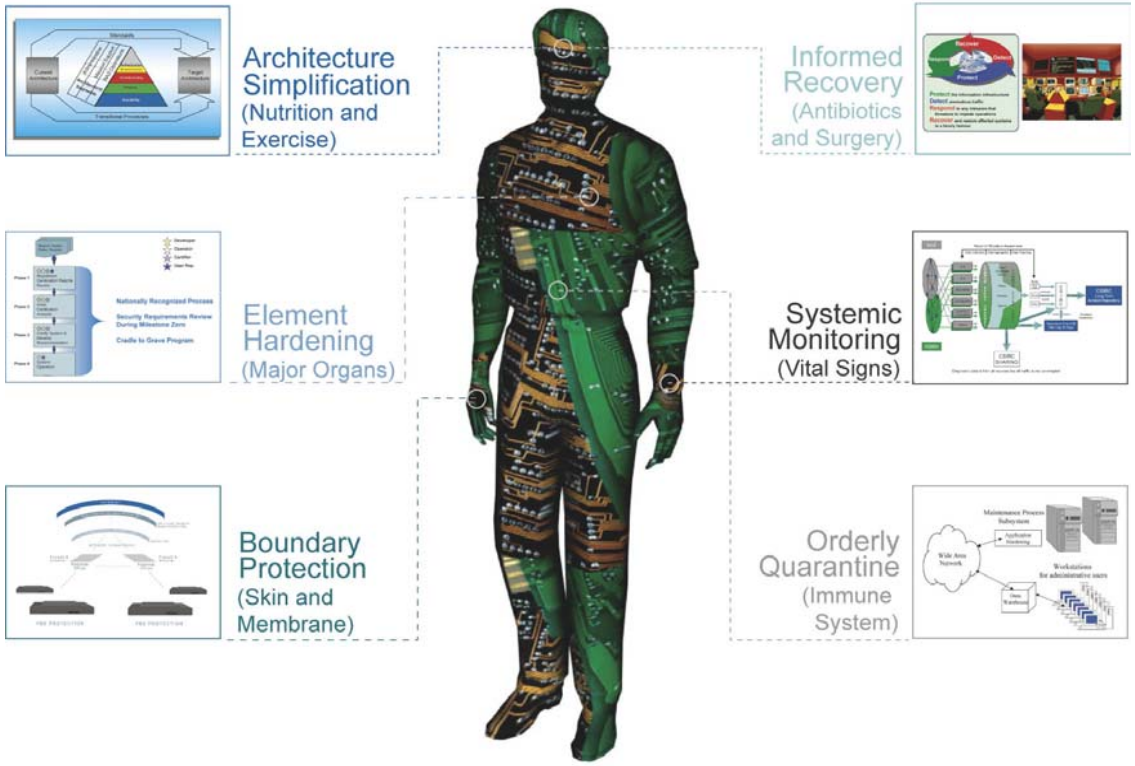
1. We will continue to implement "traditional" cyber activities around architecture simplification, element hardening, and boundary protection.
2. We will continue to help shape the nation's research agenda associated with orderly quarantine, systemic monitoring, and informed recovery. This requires

extensive interaction and partnering across a variety of educational, government, and private sector groups.

3. Finally, we will orchestrate a coordinated application of traditional and emerging cyber defense techniques to provide a comprehensive approach to cyber defense. The *android* model presents a unifying framework for addressing cyber security before, during, and after cyber attacks.

To make one final human analogy, no one can guarantee we'll never catch a cold, but we need to be sure it doesn't become a case of pneumonia. The FAA and Department of Transportation are dedicated to achieving that objective.

That concludes my remarks Mr. Chairman; I would be pleased to answer any questions you may have.



The "Android" Cyber Defense Model