Hearing before the
House Commerce Committee
Subcommittee on Oversight and Investigations

April 5, 2001

Statement of
John S. Tritak
Director
Critical Infrastructure Assurance Office

Mr. Chairman, members of the Subcommittee, it is an honor to appear before you today to discuss the status, as of the time that the Bush Administration took office,of Federal government efforts to secure internal critical systems and infrastructure within Departments andagencies. These efforts are described in some detail in the *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, January 2001*.

This Subcommittee has shown exceptional leadership on a broad range of national and economic security issues and I am grateful for the opportunity to work closely with you and the Congress to find ways to advance infrastructure assurance for all Americans. As you know, the Bush Administration currently is conducting a thorough review of our critical infrastructure protection policy. We expect the results of that review over the next couple of months. President Bush has indicated already, however, that securing our nation's critical infrastructures will be a priority of his Administration. Your decision to hold this hearing could not be more timely. We all recognize that no viable solutions will be developed or implemented without executive and legislative branches working together.

I believe the work of your subcommittee, along with that of others, will make an

important contribution to establishing a new consensuson safeguarding critical government services against deliberate cyber attacks.

Introduction

America has long depended on a complex of systems – or critical infrastructures – to assure the delivery of services vital to its national defense, economic prosperity, and social well-being. These infrastructures include telecommunications, electric power, oil and gas delivery and storage, banking and finance, transportation, and vital human and government services.

The Information Age has fundamentally altered the nature and extent of our dependency on these infrastructures. Increasingly, our government, economy, and society are being connected together into an ever expanding and interdependent digital nervous system of computers and information systems. With this interdependence come new vulnerabilities. One person with a computer, a modem, and a telephone line anywhere in the world potentially can break into sensitive government files, shut down an airport's air traffic control system, or cause a power outage in an entire region.

Events such as the 1995 bombing of the Murrah Federal Building in Oklahoma City demonstrated that the Federal government needed to address new types of threats and vulnerabilities, many of which the nation was unprepared to defend against. In response to the Murrah Building tragedy and other events, an inter-agency working group was

formed to examine the nature of the threat, our vulnerabilities, and possible long-term solutions for this aspect of our national security. The National Security Council's Critical Infrastructure Working Group (CIWG) included representatives from the defense, intelligence, and national security communities. The working group identified both physical and cyber threats and recommended formation of a Presidential Commission to address more thoroughly many of these growing concerns.

In July 1996 the President's Commission on Critical Infrastructure Protection (PCCIP) was established by Executive Order 13010. The bipartisan PCCIP included senior representatives from private industry, government, and academia; its Advisory Committee consisted of industry leaders who provided counsel to the Commission. After examining infrastructure issues for over a year, the Commission issued its report, *Critical Foundations: Protecting America's Infrastructures.* The Report reached four significant conclusions:

- First, critical infrastructure protection is central to our national defense, including national security and national economic power;
- Second, growing complexity and interdependence between critical infrastructures may create the increased risk that rather minor and routine disturbances can cascade into national security emergencies;
- Third, vulnerabilities are increasing steadily and the means to exploit weaknesses are readily available; practical measures and mechanisms, the Commission argued, must be urgently undertaken before we are confronted

with a national crisis; and

- Fourth, laying a foundation for security will depend on new forms of cooperation with the private sector, which owns and operates a majority of these critical infrastructure facilities.

Presidential Decision Directive 63

On May 22, 1998, Presidential Decision Directive 63 (PDD-63) was issued to achieve and maintain the capability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- The Federal government to perform essential national security missions and to ensure the general public health and safety;
- State and local governments to maintain order and to deliver minimum essential public services; and
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

- To achieve these ends, PDD-63 articulates a strategy of:

- Creating a public-private partnership to address the problem of information technology security;
- Raising awareness of the importance of cyber security in the government and in the private sector;

- Stimulating market forces to increase the demand for cyber security and to create standards or best practices;
- funding or facilitating research into new information technology systems with improved security inherent in their design;
- Working with educational facilities to increase the number of students specializing in cyber security; and
- Helping to prevent, mitigate, or respond to major cyber attacks by building an information sharing system among government agencies, among corporations, and between government and industry.

The Federal government's basic approach to critical infrastructure protection, as reflected in PDD-63, has been built around a strong policy preference for consensus-building and voluntary cooperation rather than regulatory actions. In an economy as complex as ours, and with technology changing as quickly as it is, cooperation offers the best and surest way to achieve our shared goals in this emerging area. However, the government's approach also recognizes the need for coordinated actions to improve its internal defenses and the nation's overall posture against these new threats.

PDD-63 called for the Federal government to produce a detailed plan to protect and defend the nation against cyber disruptions. Version 1 of this effort, entitled *The National Plan for Information Systems Protection*, was released in January 2000, and represents the first attempt by a national government to design a comprehensive approach

to protect its critical infrastructures. This initial version of the plan focused mainly on domestic efforts being undertaken by the Federal government to protect the nation's critical cyber-based infrastructures. The next version of the plan, due out this summer, will focus on the efforts of the infrastructure owners and operators, as well as the risk management industry and mainstream business.

Under PDD-63, Federal Agencies have a number of distinct responsibilities:

- All agencies are required to protect their own internal critical infrastructures, especially their cyber systems.
- Some agencies with special expertise or functional responsibilities are tasked with providing services to the government as a whole.
- A number of agencies also are charged with developing partnerships with private industry in their sectors of the economy.

Securing the Government's Critical Systems

I will focus the remainder of my remarks on the first responsibility – securing internal critical systems. Specifically, I will discuss the work of my office, the Critical Infrastructure Assurance Office, in assisting agencies to identify and prioritize these systems. I also will discuss briefly Federal Government efforts to formulate security and best practices standards that apply to information, security, and critical infrastructure assets.

Time constraints prevent me from fully describing the internal efforts of each federal agency to secure their critical systems. I urge the subcommittee to review the status reports of each Department and Agency provided in Section III of the President's January

Report. Likewise, I strongly recommend that the subcommittee study the agencies' sector partnership efforts described in Section II of the *Report.* These efforts are as important to overall national critical infrastructure assurance as the internal activities that have been undertaken within the Federal government.

Identifying Critical Federal Infrastructures and Systems: Project Matrix

In response to PDD 63, my office established Project Matrix last year to "coordinate analyses of the U.S. Government's own dependencies on critical infrastructures."

This is a government-wide issue. Federal Departments and Agencies do not operate independently of one another. Due to significant advances in information technology, the public and private sectors have become inextricably intertwined. As a result, there is limited utility in each Federal Department and Agency viewing physical and cyber security only in the context of its own organization. Project Matrix provides each Federal Department and Agency an expanded, more comprehensive, realistic, and useful view of the world within which itactually functions. The Administration, Congress, and private sector providers of the nation's critical infrastructures will require such information to implement cost efficient and effective physical and cyber security enhancement measures in the future. Project Matrix provides a common methodology and approach and allows the government to develop a clearer picture of cross-agency interdependencies.

Participating in Project Matrix helps each Federal Department and Agency identify the assets, nodes and networks, and associated infrastructure dependencies and

interdependencies that are required for itto fulfill its national security, economic stability, and critical public health and safety responsibilities to the American people. A number of Departments and Agencies refer to Project Matrix in their reports.

Project Matrix also helps each participating Federal Department and Agency:

- Identify the nodes and networks that should receive robust cyber and physical vulnerability assessments;
- Conduct near-term risk management assessments;
- Justify funding requests for high-priority security enhancement measures in the areas of physical security, information system security, industrial security, emergency preparedness, counter-intelligence, counter-terrorism; and
- Review actual business processes to better understand and improve the efficiencies of its organization's functions and information technology architectures.

Project Matrix involves a three-step process. In Step 1, the Project Matrix team identifies and prioritizes each Federal Department's and Agency's PDD 63 relevant assets. In Step 2, the team provides a business process topology on, and identifies significant points of failure associated with, each Department's or Agency's most critical assets. In Step 3, the team identifies the infrastructure dependencies associated with select assets identified in Step 1 and analyzed in-depth in Step 2.

In FY 2001, the Project Matrix team will complete the documentation of its entire analytical process for use throughout the public and private sectors, improve its Step One automated data collection tool, and develop compatible automated Step

Two and Three tools.

Integrating Security into the Capital Planning and Budget Processes

In February 2000, OMB issued important new guidance to the agencies on incorporating and funding security in information technology investments. In brief, this policy states that funding will not be provided for agency requests that fail to demonstrate how security is built into and funded as part of each system.

This policy carries through on the requirements of the Clinger-Cohen Act of 1996 and emphasizes that security must be incorporated in and practiced throughout the life cycle of each agency's system and program. To accomplish this, beginning with the FY 2002 budget, each agency budget request to OMB for information technology funding must, among other things:

- Demonstrate life cycle security costs for each system;
- Include a security plan that complies with applicable policy;
- Show specific methods used to ensure that risks are understood, continually assessed, and effectively controlled; and
- Demonstrate that security is an integral part of the agency's enterprise architecture including interdependencies and interrelationships.

The Government Information Security Reform Act

On October 30, 2000 the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform (Security Act)." The security provision amends the Paperwork

Reduction Act of 1995 (44 U.S.C. Chapter 35) and primarily addresses the program management and program evaluation aspects of security.

In concert with OMB policy, the Security Act requires agencies to incorporate and practice risk-based and cost-effective security throughout the life cycle of each agency system and thus firmly ties security to the agencies' capital planning and budget processes.

The Security Act also requires on an annual basis:

- Agency program reviews;
- Inspector General evaluations of agency security programs;
- Agency reports to OMB; and
- An OMB report to Congress.

The annual review and reporting requirements will promote consistent, ongoing assessments of government security performance. Recently a uniform method for agency program reviews has been developed.

The CIO and CFO Councils: Standards And Best Practices

Standardizing the security controls for government systems has a conceptual appeal because it can reduce the complexity and expense of developing, implementing, and monitoring security on a system-by-system basis. This is increasingly important given the government's shortage of expert information security personnel. Government computer security almost certainly would improve if specific standards were prescribed and implemented for each government information system.

However, specific standards for all systems -- a "one-size-fits-all" security

approach--may not accommodate the vastly different operational requirements of each information system and could unnecessarily impede business operations. Executive branch agencies operate more than 26,000 major information systems, many of which directly interact with the public, industry, or State and local governments. Just as each system has its own unique operational requirements, so too are its security requirements unique.

The CIO Council and the CFO Council recognize both the benefits and potential problems with standardized security approaches. They have undertaken the following important initiatives:

Security Benchmark for Agency Financial Systems: The CFO Council is reviewing the viability of establishing a security benchmark or standard security expectation for agency financial systems.

Securing Electronic Government Transactions to the Public – Resource Guide: The CIO Council, the CFO Council, and the Information Technology Association of America are working together to develop a benchmark for risk-based, cost-effective security for three types of electronic government services:

- Web-based information services;
- Government procurement; and
- Financial transactions with the public.

A resource guide for securing electronic transactions with the public will be released in 2001 to assist agency CIOs in promoting electronic government initiatives within their agencies. Together with the CFO Council initiative for agency financial

systems, this effort may prove to be an effective pilot for establishing similar benchmarks for other discrete classes of programs and information systems.

Best Security Practices: The CIO Council, led by the U.S. Agency for International Development and NIST, has developed a web-based repository of sound Federal agency security practices that have worked in the real world. The CIO Council's Best Security Practices initiative collects, documents, and disseminates these practices to help agencies reduce the cost of developing and testing new security controls, improve the speed of implementation, and increase the quality of their security programs.

The goal is to populate the repository with more than 100 practices by mid 2001 and continually expand offerings from then on. In their guidance to the agencies on implementing the Government Information Security Reform Act, OMB has instructed agencies to use the CIO Council's best practices initiative to fulfill the new act's requirement to share best practices.

Measuring Performance -- Federal Information Technology Security Assessment Framework: Over the past year, the CIO Council, working with NIST, OMB, and the GAO, developed the Federal Information Technology Security Assessment Framework. The framework, issued in December 2000, provides agencies with a self-assessment methodology to determine the current status of their security programs and, where necessary, establish a target for improvement. In developing the framework, the CIO Council recognizes that the security needs for the tens of thousands of Federal information systems differ and must be addressed in different ways.

The framework comprises five levels to guide agency self assessments and to

assist them in prioritizing efforts for improvement:

- Level 1 reflects a documented security policy;
- Level 2 shows documented procedures and controls to implement the policy;
- Level 3 indicates that the procedures and controls have in fact been implemented;
- Level 4 shows that the procedures and controls are continually tested and reviewed; and
- Level 5 demonstrates that procedures and controls are fully integrated into a comprehensive program.

Each level represents a more complete and effective security program. Agencies should bring all systems and programs to level 4 and ultimately level 5. OMB and the CIO Council have alerted agencies that when individual systems do not meet the framework's level 4 requirements, the system may not meet OMB's security funding criteria.

As mentioned earlier, the new Government Information Security Reform Act emphasizes the importance of assessing security effectiveness and requires annual agency reporting to OMB of the results of the agency security reviews. OMB has instructed agencies to use the framework to fulfill their assessment and reporting obligations under the Security Act.

Conclusion

While much has been accomplished in recent years, much more needs to be done to ensure our critical government systems are adequately protected from cyber attack. I look forward to working with members of this subcommittee, and the entire Congress, as we address the challenges ahead. I look forward to your questions.

--- oOo --