POLICY ISSUE
(INFORMATION)

April 14, 2000 SECY-00-0088

FOR: The Commissioners

FROM: Stuart Reiter
Acting Chief Information Officer

SUBJECT: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION

PURPOSE:

To inform the Commission of the National Plan for Information Systems Protection

BACKGROUND:

President Clinton recently released the National Plan for Information Systems Protection, Version 1.0. It is the first major element of a more comprehensive effort to protect critical information systems from cyber-attack. The plan responds to Presidential Directive 63 (PDD-63) which directed its development.

DISCUSSION:

The National Plan for Information Systems Protection largely focuses on domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures. The plan represents the starting point for discussions with private sector owners and operators of critical infrastructures, and other interested parties. The purpose of these discussions is to refine the plan so that together the public and private sectors can overcome the unique challenge to our national security that the Federal Government cannot meet alone.

The plan is built around three major objectives:

1. Prepare and Prevent: Those steps necessary to minimize the possibility of a significant and successful attack on the nation's critical information networks, and build an infrastructure that remains effective in the face of such attacks.

2. Detect and Respond: Those actions required to identify and assess an attack in a timely way, and then to contain the attack, quickly recover from it, and reconstitute affected systems.

Contact:
Jesse Cloud, OCIO
415-7674

3. Build Strong Foundations: The things we must do as a nation to create and nourish the people, organizations, laws and traditions which will make us better to prepare and prevent, detect and respond to attacks on the nation's critical information networks.

The plan proposes ten programs for achieving these objectives. They are attached for your information.

Attachment: As stated

/RA/

Stuart Reiter
Acting Chief Information Officer

Attachment

National Plan Information Systems Protection Programs

Program 1: Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities

"First, know thyself."

The First Program is for Government and the Private sector to identify significant assets, interdependencies, and vulnerabilities of critical information networks to attack, then develop and implement realistic programs to remedy the vulnerabilities, while continuously updating the assessment and remediation effort.

Program 2: Detect Attacks and Unauthorized Intrusions

"Today, we don't even know when we are being attacked."

The Second Program installs multi-layered protection on sensitive computer systems, including advanced firewalls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers (first in DOD, then the Federal Intrusion Detection Network [FID Net] in coordination with other Federal Agencies) will receive warnings from these detection devices, as well as Computer Emergency Response Teams (CERTs) and other means, in order to analyze the attacks and assist sites in defeating attacks.

Program 3: Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law.

"People form governments to defend themselves from foreign enemies and domestic criminals."

The Third Program assists, transforms, and strengthens U.S. law enforcement and intelligence agencies to be able to deal with a new kind of threat and a new kind of criminal, one that acts against computer networks.

Program 4: Share Attack Warnings and Information in a Timely Manner

"An attack on one shall be considered an attack on all."

The Fourth Program is to improve Federal information sharing by encouraging the establishment of state and Federal information sharing and analysis centers and to remove barriers to information sharing so companies who wish to share system vulnerabilities with the government would not be deterred because information disclosed to the government could be subject to public disclosure.

Program 5: Create Capabilities for Response, Reconstitution, and Recovery
"...isolate and minimize damage....restore required capabilities rapidly"

The Fifth Program is to limit an attack while it is underway and to build into corporate and agency continuity and recovery plans the ability to deal with information attacks.

Program 6: Enhance Research and Development in support <u>of Programs 1-5</u>

"Information Technology is progressing at the speed of Internet years, four for every calendar year."

The Sixth Program systematically establishes research requirements and priorities needed to implement the plan, ensures their funding, and creates a system to ensure that our information security technology stays abreast with changes in the threat and in overall information systems.

Program 7: Train and Employ Adequate Numbers of Information Security Specialists

"We just don't have the trained people."

The Seventh Program surveys the numbers of people and the skills required for information security specialists within the Federal Government and nationwide, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.

Program 8: Outreach to Make Americans Aware of the Need for Improved Cyber-Security

"Action follows understanding."

The Eighth Program will explain publicity the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyber attack.

Program 9: Adopt Legislation and Appropriations in Support of Programs 1-8

"Just as the Government must form a partnership with private industry, the Executive Branch and Congress must work closely together to defend our Nation's critical infrastructures."

The Ninth Program develops the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation between the Federal Government, including Congress, and private industry.

Program 10: In Every Step and Component of the Plan, Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to the Protection of Proprietary Data.

"...the right of the people to be secure in their persons, houses, papers, and effects..."

The Tenth Program is incorporated in every other program and is making what we do in the protection of critical cyber systems conform to Constitutional and other legal rights.

3. Build Strong Foundations: The things we must do as a nation to create and nourish the people, organizations, laws and traditions which will make us better to prepare and prevent, detect and respond to attacks on the nation's critical information networks.

The plan proposes ten programs for achieving these objectives. They are attached for your information.

Attachment: As stated

Stuart Reiter
Acting Chief Information Officer

Distribution:
RidsOcio
RidsOcioPrmdPab

Accession Number: ML003698315
Title of Document: National Plan for Information Systems Protection, Version 1; Highlights for the Commission

To receive a copy of this document, indicate in the box: "**C**" = Copy without attachment/enclosure "**E**" = Copy with attachment/enclosure "**N**" = No copy

OFFICE	**OCIO**	**C**	**OCIO/PRMD**	**C**	**OCIO**	**C**		
NAME	**D.Grimsley:DHG**		**J.Cloud: JC**		**S.Reiter SR**			
DATE	**03/31/00**		**04/05/00**		**04/14/00**		**/ /00**	

OFFICIAL RECORD COPY