NSTISSD No. 503
August 30, 1993

NSTISS
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

INCIDENT RESPONSE AND VULNERABILITY REPORTING FOR NATIONAL SECURITY SYSTEMS

~~FOR OFFICIAL USE ONLY~~

NSTISSC
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

CHAIRMAN

August 30, 1993

FOREWORD

1. In response to recent attempts to exploit and disrupt national security systems, as defined in National Security Directive 42, dated July 5, 1990, this directive sets up an essential program for coordinating countermeasures against such incidents. The National Security Information Systems Incident Program (NSISIP) puts in place a National Security Incident Response Center (NSIRC) whose primary purpose is to provide expert assistance in isolating, containing, and eliminating incidents that threaten the integrity, availability, or confidentiality of national security systems.

2. The NSISIP also calls on U.S. Government departments and agencies involved with national security systems to establish a Security Incident Response Capability (SIRC). A SIRC provides incident response service for its constituency at the agency level, whereas the NSIRC responds to requests from SIRCs for expert assistance in handling incidents that are beyond the technical capability or organizational scope of a single constituency. SIRCs also use the NSISIP to share information with the NSIRC about incidents that are likely to threaten other national security systems.

3. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this directive from:

Executive Secretariat
National Security Telecommunications and
Information Systems Security Committee
National Security Agency
Fort George G. Meade, MD 20755-6000

4. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer representative regarding distribution of this document.

Mr. Emmett Paige, Jr.

(b) (6)

INCIDENT RESPONSE AND VULNERABILITY REPORTING FOR NATIONAL SECURITY SYSTEMS

SECTION I - PURPOSE

1. This Directive establishes the National Security Information Systems Incident Program (NSISIP) to provide a strategy for responding to information systems security incidents and vulnerabilities among national security systems, as defined in National Security Directive 42, dated July 5 1990.

SECTION II - SCOPE AND APPLICABILITY

2. The NSISIP focuses on security incidents and vulnerabilities that threaten national security systems. This program is applicable to all U.S. Government departments and agencies and their contractors that acquire, develop, use, maintain, or dispose of national security systems.

SECTION III - REFERENCES

3. NSTISSP 5, National Policy for Incident Response and Vulnerability Reporting for National Security Systems, dated August 30, 1993.

4. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated June 5, 1992.

5. National Security Directive 42, dated July 5, 1990.

SECTION IV - DEFINITIONS

6. For the purpose of this document, the following terms are defined:

a. Technical Vulnerability - a hardware, firmware, or software weakness or design deficiency that leaves an information system open to potential exploitation, either externally or internally, thereby resulting in risk of compromise of information, alteration of information, or denial of service.

b. Administrative Vulnerability - a security weakness caused by incorrect or inadequate implementation of a system's existing security features by the system administrator, security officer, or users. An administrative vulnerability is not the result of a design deficiency but is characterized by the fact

that the full correction of the vulnerability is possible through a change in the implementation of the system or the establishment of a special administrative or security procedure for the system administrators and users.

c. Security Incident - an attempt to exploit a national security system such that the actual or potential adverse effects may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial of service. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code. (A security incident may also involve a violation of law. If a violation of law is evident or suspected, the incident must be reported to both security and law enforcement organizations for appropriate action.)

d. Security Incident Response - actions conducted to resolve information systems security incidents and protect national security systems.

SECTION V - OBJECTIVES

7. The objectives of the NSISIP are to coordinate national security systems vulnerability and incident reporting and responses, while facilitating:

a. cooperation among appropriate organizations and agencies in sharing incident, vulnerability, threat, and countermeasures information concerning national security systems;

b. effective and timely response to security incidents on national security systems;

c. development and use of incident response methods, countermeasures, and technologies; and

d. timely reporting of violations of law to appropriate law enforcement agencies.

SECTION VI - CLASSIFICATION GUIDANCE FOR VULNERABILITY AND INCIDENT REPORTS

8. Protection of Vulnerability Reports

a. Vulnerability reports shall be protected from public disclosure in accordance with applicable statutes, directives, executive orders, and regulations.

b. Vulnerability reports for commercial off-the-shelf systems or components (hardware, firmware, or software) shall be unclassified and marked For Official Use Only (FOUO).

c. Reports of vulnerabilities in national security systems that are not available for purchase by the general public shall be unclassified unless the exploitation of the vulnerability would result in the compromise of classified information or would present a significant negative impact on a national security organizational mission. In those instances, the originator may place a maximum classification on the vulnerability report equal to the level of the classified information processed on that system.

9. Protection of Incident Reports

a. Incident reports shall be protected from public disclosure in accordance with applicable statutes, directives, executive orders, and regulations.

b. Incident reports shall be unclassified and marked For Official Use Only (FOUO) unless the exploitation of the information in the incident report would result in the compromise of classified information or would present a significant negative impact on a national security organizational mission.

SECTION VII - RESPONSIBILITIES

10. The National Manager, in fulfilling responsibilities contained in National Security Directive 42, shall oversee the administration of this program.

11. The administrator of this program shall be responsible to the National Manager for:

a. establishing and operating a National Security Incident Response Center (NSIRC) to centrally coordinate actions involving security incidents and vulnerabilities that threaten national security systems;

b. developing, reviewing, and revising procedures and guidance for this program;

c. reviewing all reported national security systems vulnerabilities and incidents and evaluating the requirement for and extent of follow-up actions;

d. facilitating the reporting of security incidents involving violations of law to the appropriate authority;

e. facilitating and coordinating the identification and/or development of appropriate countermeasures;

f. providing effective and timely response support to security incidents as needed to supplement agency activities;

g. facilitating the development and use of specialized technical tools;

h. facilitating cooperation with organizations that handle information systems incident responses that occur outside the national security community;

i. acting as the focal point for coordinating the national level response to security incidents; and

j. developing and disseminating any NSISIP reports that may be required at the national level.

12. Heads of U.S. Government departments and agencies using national security systems shall:

a. establish a security incident response capability (SIRC) to meet the objectives of this program;

b. identify to the program administrator an individual to act as their organization's focal point for this program;

c. ensure the direct reporting of violations of law to the appropriate authority; and

d. develop organizational policies, procedures and guidance to implement this program.