CNSSP No. 22
January 2012

Policy
on
Information Assurance
Risk Management
for
National Security Systems

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION

CHAIR

FOREWORD

1. The Committee on National Security Systems (CNSS) Policy (CNSSP) No. 22 provides the guidance and responsibilities for establishing an integrated, organization-wide Information Assurance (IA) risk management program to achieve and maintain an acceptable level of IA risk for organizations that own, operate, or maintain National Security Systems (NSS). Implementing an IA risk management program provides a framework for decision makers to evaluate and prioritize IA risks along with other critical risks in order to determine the appropriate response to those risks. In addition, organizations must have confidence that the information they share will be adequately protected by receiving organizations. Adherence to this policy enables leaders within the organization to make informed, risk-based decisions and fosters trust among organizations leading to the confidence needed to share information.

2. As part of the Joint Task Force Transformation Initiative Working Group, the CNSS is working with representatives from the Civil, Defense, and Intelligence Community to produce a unified information security framework. The CNSS intends to adopt National Institute of Standards and Technology (NIST) issuances where applicable. Additional CNSS issuances will occur only when the needs of NSS are not sufficiently addressed in a NIST document. Annex B identifies the guidance documents, which includes NIST Special Publications (SP), for establishing an organization-wide risk management program. Annex B will be updated as necessary.

3. This policy is available from the CNSS Secretariat, as noted below, or the CNSS website: http://www.cnss.gov.

/s/
TERESA M. TAKAI

INFORMATION ASSURANCE RISK MANAGEMENT FOR NATIONAL SECURITY SYSTEMS

SECTION I—PURPOSE

1. CNSSP No. 22 requires the implementation of an integrated organization-wide program for managing IA risk to organizational operations (i.e., mission, functions, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of National Security Systems (NSS). Risk management is a comprehensive process that requires organizations to frame risk, assess risk, respond to risk once determined, and monitor risk on an ongoing basis. This policy will be implemented based upon guidance found in the documents listed in Annex B, which provide a detailed approach to IA risk management. Upon this revision of CNSSP No. 22, CNSS Policy No. 6, "National Policy on Certification and Accreditation of National Security Systems," dated October 2005, and National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 1000, "National Information Assurance Certification and Accreditation Process (NIACAP)," dated April 2000 will be canceled.

SECTION II—AUTHORITY

2. CNSSP No. 22 is issued pursuant to National Security Directive No. 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated 5 July 1990 (Reference a), which outlines the roles and responsibilities for securing NSS, and applicable sections of the Federal Information Security Management Act (FISMA) of 2002 (Reference b). Nothing in this Directive shall alter or supersede the authorities of the Director of National Intelligence.

SECTION III—SCOPE

3. CNSSP No. 22 is applicable to all departments and agencies of the United States Government (USG), as defined in Reference b, its employees, and contractors, who own, operate, or maintain NSS.

SECTION IV—POLICY

4. It is the CNSS policy that all organizations that own, operate, or maintain NSS ensure organizational operations by establishing and implementing an IA risk management program for their NSS that will:

a. Establish a risk executive (function) to ensure the program is consistent with the provisions of NIST Special Publication (SP) 800-39 (Reference d); provide guidance to and oversight of the organization's risk management program and development of the risk management strategy; communicate organization-wide threat, vulnerability, and risk-related information; and provide a strategic view for managing IA risk throughout the organization.

b. Establish processes to identify IA risks from an organization-wide perspective; determine which risks are acceptable; achieve operational effectiveness by selecting, implementing, and assessing safeguards and countermeasures to adequately mitigate unacceptable risks; and take any additional corrective actions as necessary.

c. Establish processes to deploy security controls throughout the organization consistent with its enterprise architecture, taking advantage of the common control concept as described in NIST SP 800-37 (Reference e) to cost-effectively implement IA security controls within the organization.

d. Establish processes to develop and maintain existing organizational policies and procedures to integrate IA risk management throughout the information system lifecycle (e.g., acquisition, design, development, integration, distribution, operation, maintenance, and retirement).

SECTION V—RESPONSIBILITIES

5. In accordance with FISMA, heads of Federal departments and agencies, to include independent bureaus and offices, are responsible for the overall IA risk management within their organization and shall:

a. Establish an IA risk management program to support the implementation of CNSSP No. 22 including Annex B issuances as appropriate.

b. Ensure that organizational policies and practices integrate IA risk management throughout the information systems lifecycle (e.g., acquisition, design, development, integration, distribution, operation, maintenance, and retirement).

c. Ensure IA risk management processes are efficient, effective, and maximize the assurance of organizational operations.

d. Ensure ongoing review of threats, vulnerabilities, technologies, and mission changes to assess their impact to the organizational risk posture.

e. Ensure that NSS-related IA risk issues that cannot be resolved between or among organizations are referred to the appropriate governance body for resolution in accordance with DoD, IC, or Federal policy.

f. Ensure a plan is developed documenting the department/agency's schedule,

including milestone dates, for implementing CNSSP No. 22. The plan shall be developed within 6 months of the approval of CNSSP No. 22. Full implementation shall be completed no later than 3 years after CNSSP No. 22 is approved.

SECTION VI—DEFINITIONS

6. All terms used in this policy are defined in CNSSI No. 4009 (Reference c).

SECTION VII - REFERENCES

7. References are listed in Annex A. Future updates to referenced documents shall be applicable to this policy.

Enclosures:
ANNEX A - References
ANNEX B – Implementation Guidance

ANNEX A

REFERENCES

a. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, July 5, 1990.

b. Public Law 107-347 [H.R. 2458], codified at 44 U.S.C. § et seq., *The E-Government Act of 2002, Title III, the Federal Information Security Management Act of 2002*, December 17, 2002.

c. Committee for National Security Systems Instruction 4009 (CNSSI 4009), *National Information Assurance Glossary*, April 2010.

d. NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, March 2011.

e. NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

f. Executive Order 12333, United States Intelligence Activities, as amended, December 4, 1981.

ANNEX B

IMPLEMENTATION GUIDANCE

The following documents are applicable to the national security community to establish an organization-wide risk management program.

a. NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. This document, as written, is applicable to organizations that employ NSS.

b. NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection, implementation, security control assessment, information system authorization, and security control monitoring. This document, as written, is applicable to the organizations that employ NSS.

c. NIST SP 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*, provides guidance on the process for selecting security controls, as well as providing the security controls applicable to all federal government information systems. Portions of this document are applicable to the national security community, as described in CNSSI 1253.

d. CNSS Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems*, adopts the security controls catalogued in NIST SP 800-53, and concepts from Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, as adapted for use with NSS. It also provides guidance for categorizing NSS and the information it processes, security control selection criteria for the controls, baseline sets of controls for NSS based on the system categorization and security control selection criteria, and parameter values for several security controls.

e. NIST SP 800-53A, Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems*, provides guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the federal government. This document, as written, is applicable to organizations that employ NSS.