Committee on National Security Systems

CNSS Policy No. 22
February 2009

INFORMATION ASSURANCE RISK MANAGEMENT POLICY FOR NATIONAL SECURITY SYSTEMS

This document prescribes minimum standards.
Your department or agency may require further implementation.

CHAIR

FOREWORD

1. Information Assurance (IA) Risk Management is a process employed by an organization to achieve and maintain an acceptable level of IA risk. This document establishes the requirements for enterprise IA risk management within the national security community which requires a holistic view of the IA risks to National Security Systems (NSS) operating within the enterprise using disciplined processes, methods, and tools. It provides a framework for decision makers to continuously evaluate and prioritize IA risks in order to accept or recommend strategies to remediate or mitigate those risks to an acceptable level. Risk assessment is the process of determining the extent to which an entity is threatened; that is, determining the likelihood of potential adverse circumstances or events and the resulting harm to or impact on organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. When operating local information systems or communicating information between government organizations, it is the responsibility of the organization to ensure the security of that information and the information system on which it is stored, processed, or transmitted. To encourage agencies to share information, they must have confidence that the information will be adequately protected by the receiving organization. This confidence is gained through the use of universally accepted and implemented risk management activities, with demonstrated performance over time. This process provides organizations the confidence to share information at the appropriate level of trust.

2. This policy derives its authority from National Security Directive 42 (NSD-42) (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).

3. The Committee on National Security Systems (CNSS) Secretariat is tracking the status of the Member and Observer organizations' implementation of new/revised CNSS Issuances in order to create an Issuance Compliance Report. The Secretariat will oversee and administer this report process, which will be initiated six months following approval of this policy.

4. Additional copies of this policy may be obtained from the Director of National Intelligence, the CNSS Secretariat, the CNSS or DNI websites: www.cnss.gov or http://www.dni.gov.

5. The CNSS is developing several instructions that will provide guidance for implementing the Risk Management Program outlined in this policy. They include guidance on categorizing information and information systems (CNSSI No. 1199), a Security Controls Catalog (CNSSI No. 1253), a Guide to Assessing Security Controls (CNSSI No. 1253a) and a guide for assessing risk (CNSSI No. 1230). Until such time as these instructions are approved and published, use existing policies and guidance.

/s/
JOHN G. GRIMES

INFORMATION ASSURANCE

RISK MANAGEMENT POLICY

FOR

NATIONAL SECURITY SYSTEMS

SECTION I –PURPOSE AND SCOPE

1. The principal goal of the National Security Community Information Assurance (IA) risk management approach is to enhance the mission assurance posture of the National Security Community by protecting its information assets. An IA Risk Management Program enables a Federal Department, Agency, Bureau or Office to successfully assess IA risks arising from information systems, prioritize those risks, implement security controls to mitigate the risks and meet their information assurance priorities, assess the operational performance and effectiveness of those controls, and maintain the appropriate level of trust that enables the sharing of national security information with other enterprises.

2. This policy applies to all Federal Government departments, agencies, bureaus, and offices, including their supporting contractors and agents, that operate, use, or manage National Security Systems (NSS), as defined in Reference B.

SECTION II – REFERENCES

3. References are listed in ANNEX A. Future updates to referenced documents shall be considered applicable to this policy.

SECTION III – DEFINITIONS

4. The following definition is provided to clarify the use of specific terms contained in this policy. All other terms used in this policy are defined in Reference C.

Information Assurance Risk Management Framework (RMF) – Provides organizations with a disciplined, structured, flexible, and repeatable process for managing risk related to the operation and use of information systems.

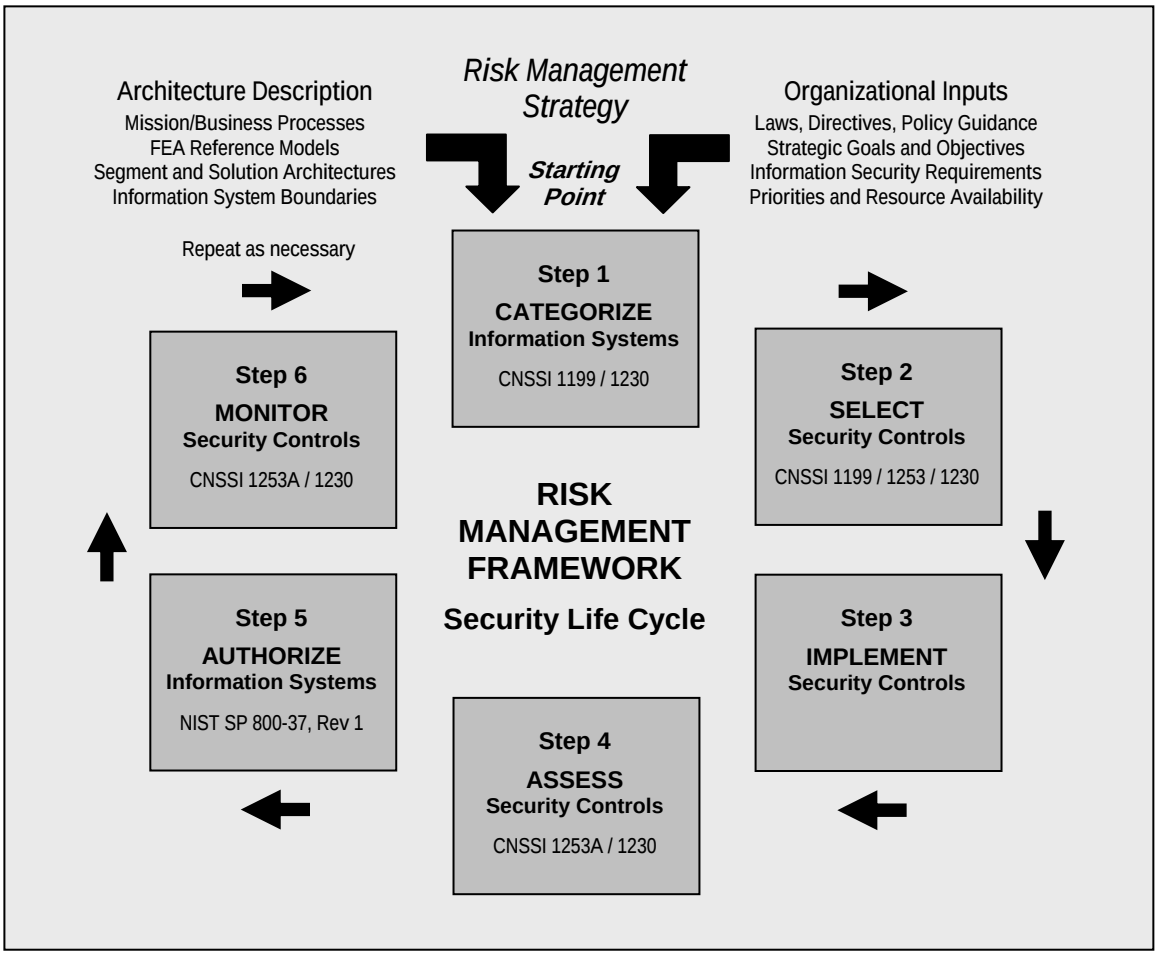

Figure 1 – Information Assurance Risk Management Framework

SECTION IV – POLICY

5. Each Enterprise within the NSS community shall establish and implement an IA Risk Management Program in accordance with this policy. The program will:

a. Identify IA risks starting at the organization level; determine what risks are acceptable; achieve operational effectiveness by selecting, implementing, and assessing safeguards and countermeasures to adequately mitigate unacceptable risks; and take additional corrective actions as necessary.

b. Focus on the total set of information systems that is supporting the enterprise in order to assess risk to the enterprise and to allocate controls most effectively across the enterprise.

c. Establish a senior risk executive function at the Enterprise level to ensure the program is consistent with the provisions of Reference B and provide guidance and oversight of risk assessments and risk decisions. The guidance and oversight shall consider risk across the organization (e.g., acquisition, financial, physical, personnel, mission, technology, information, information system, etc.). This function may be assigned to an individual or to a formal board as deemed appropriate by the head of the implementing organization.

d. Integrate defense-in-breadth IA risk management into organizational and governance structures, planning, and operational processes to complement existing defense-in-depth activities.

e. Establish, implement, and manage programs necessary to ensure that the requirements of this policy are achieved and that plans, programs, and CNSS issuances that implement this policy are fully supported.

f. Ensure that the provisions of this policy are reflected as requirements in requests for proposals and resulting contracts, as applicable.

g. Develop or modify existing organizational policies and procedures to integrate IA risk management with the information system lifecycle (including acquisition, design, development, integration, distribution, operation, maintenance, and retirement).

h. Ensure the review of current IA practices and procedures to integrate, adopt, and implement on a continuous basis, lifecycle defense-in-breadth mitigation strategies with regard to all NSS.

i. Establish and implement initial and annual refresher IA risk management training, education, and awareness. This training should include appropriate risk assessment training for all levels within the organization, and in particular all organizational business area heads, program managers, contracting officers, and information system security engineers. The training will also incorporate defense-in-breadth IA risk management development topics into IA training in accordance with Reference D.

j. Ensure that the principles set forth in Reference E, the *National Operations Security Program*, are included in the IA risk management program.

SECTION V – RESPONSIBILITIES

6. Heads of Federal Departments and Agencies, to include independent Bureaus and Offices shall be accountable for the overall IA risk management performance of their enterprises and:

a. Develop, fund, implement, and manage an Information Assurance Risk Management Program to ensure that the goals of this policy are achieved and that the plans, programs, and CNSS issuances that implement this policy are fully implemented.

b. Review, at least annually, existing IA risk management processes to ensure compliance with this policy.

c. Ensure that all NSS, to include new acquisitions, developments, and legacy systems, comply with this policy.

d. Ensure risk assessments are conducted from an enterprise perspective, conducting top-down assessments and analyzing the compilation of risks identified by individual information system owners.

e. Ensure that enterprise risk assessments fully consider strategic, mission, business, and financial impacts to the enterprise and are not solely based on the information security aspects of the program.

f. Ensure that NSS-related IA risk issues that cannot be resolved between or among organizations within an Enterprise are referred to the appropriate governance body for resolution (e.g., the Department of Defense DISN/GIG Flag Panel, the Intelligence Community Information Technology Governance Board, the Program Manager-Information Sharing Environment Information Sharing Council).

g. Submit unresolved IA risk issues affecting two or more CNSS members to the full CNSS Committee for resolution. Unresolved IA risk issues must be submitted in writing to the CNSS Secretariat through the organization's CNSS Committee Member and include supporting documentation that will assist the CNSS Committee in its deliberations and conflict resolution. The CNSS Secretariat shall process the request consistent with CNSS Committee Member voting procedures.

h. Provide relevant IA risk management information to parties that are affected by their risk management decisions.

i. Promote Information Assurance and IA risk awareness.

j. Ensure continuous review of current threats, vulnerabilities, technologies, and mission changes for impact on organizational risk posture.

k. Require a formal Enterprise-level Plan of Actions and Milestones (POA&M) containing: (i) systemic information system and organizational security weaknesses and deficiencies; (ii) risks relating to the identified weaknesses and deficiencies requiring further mitigation; and (iii) specific actions to mitigate identified risks.

Enclosure:
ANNEX A - References

ANNEX A

February 2009

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*, June 2006

D. CNSSI No. 4016, *National Information Assurance Training Standard for Risk Analysts*, November 2005

E. National Security Decision Directive Number 298, *National Operations Security Program*, January 22, 1988