Committee on National Security Systems

CNSS Policy No. 21
March 2007

National Information Assurance Policy
on
Enterprise Architectures for
National Security Systems

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

CHAIR

FOREWORD

1. Public Law 107-347, E.-Government Act of 2002, requires the development of enterprise architectures within and across the Federal Government, and the provision of information security protections commensurate with the risk and magnitude of the harm resulting from information systems' corruption. Information Assurance (IA) is the protection of information in information systems (IS). IA provides a level of security to assure the right information gets to the right people at the right time by ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of that information. When communicating National Security Information (NSI) between government organizations, it is the responsibility of both parties to ensure the security of that information. This is accomplished through the inclusion of coordinated IA requirements in those organizations' enterprise architectures.

2. However, in today's environment, information systems that handle NSI are operating in different Federal Departments and Agencies whose security needs and architectural requirements vary. These combined factors present great hurdles in simultaneously achieving the necessary degree of information assurance with the greatest degree of information sharing, as the national security community moves towards a net-centric environment.

3. This policy is the central policy to coordinate and clarify the development and integration of IA components of enterprise architectures across the CNSS community, focusing on the Federal Enterprise Architecture (FEA) as the framework to make this integration possible. It enumerates responsibilities and requirements for Federal Departments and Agencies in their development of collaborative, integrated IA components of enterprise architectures that handle NSI.

4. In accordance with the Federal Information Security Management Act (FISMA) of 2002, the Committee on National Security Systems (CNSS) Secretariat has initiated an Issuance Compliance Process for reporting annual status of Department and Agency implementation of new/revised CNSS Issuances. The first report for the attached policy is due six months following its issuance.

5. Additional copies of this policy may be obtained from the Secretariat or at the CNSS website: www.cnss.gov.

/s/
JOHN G. GRIMES

NATIONAL INFORMATION ASSURANCE POLICY ON ENTERPRISE ARCHITECTURES FOR NATIONAL SECURITY SYSTEMS

SECTION I – SCOPE

1. This policy applies to all Federal Government departments, agencies, employees, and contractors that develop enterprise architectures (EA), as defined in reference a, which describe the collection, generation, processing, storage, displaying, transmission, or receipt of national security information (NSI), as defined in reference b, herein referred to as NSI Components of EA.

SECTION II – REFERENCES

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

SECTION III – DEFINITIONS

3. Definitions used in this policy are contained within reference c, ANNEX B, or other references when specifically indicated.

SECTION IV – POLICY

4. Federal Department and Agency EAs shall integrate IA capabilities to mitigate risks associated with NSI. The development of integrated, secured, and assured EAs is key in the support of achieving the information sharing goals set forth in references d and e. The proper application of IA, integrated from the inception of EA development, is an essential contributor to achieving information sharing goals for the national security community.

5. EAs that integrate IA shall be developed by all Federal Departments and Agencies, in accordance with references a, f, g and the Federal Enterprise Architecture (FEA)[1], under the oversight of the Office of Management and Budget (OMB).

6. Federal Departments' and Agencies' EAs shall be documented and provided to OMB, in accordance with reference h. Timely feedback on EAs shall be provided to OMB using the established feedback mechanisms defined in references i and j. This will ensure that the FEA is being followed, and that there is consistency across Federal EAs.

[1] The background, structure, process, and requirements for development, assessment, and maintenance of FEA compliant EAs are found on the Federal E-Gov Website at http://www.whitehouse.gov/omb/egov.

7. For existing Federal Department and Agency EA frameworks and the EAs developed from them, the Federal Transition Framework (FTF), reference k, shall be applied to identify opportunities for cross-agency collaboration related to IA integration into EAs.

8. Security controls shall be incorporated at the component, system, service, and application levels of EAs, including plans to manage risk, protect privacy, and provide availability, integrity, authentication, confidentiality, and non-repudiation as part of an integrated IA approach.

9. A Security and Privacy Profile (SPP) shall be developed, in accordance with reference l, for each Federal Department and Agency EA to define IA requirements. The security requirements associated with NSI shall be properly and thoroughly described within developed SPPs.

10. To ensure that the SPP sufficiently addresses IA integration for NSI Components of EA, the SPP and related sections of the FEA shall be reviewed and modified to the extent necessary. This review and modification cycle shall occur as an integrated part of the maintenance process described in reference i.

11. Performance metrics and information training programs shall be developed in accordance with reference m, and shall include coherent and integrated approaches to IA. Standards and guidelines developed for NSI Components of EA shall be complementary with the standards and guidelines developed by the National Institute of Standards and Technology (NIST) for non-NSS.

12. NSI Components of EA shall be funded and adequately addressed, based on appropriate risk assessments, throughout the EA lifecycle. Federal Departments and Agencies shall incorporate funding for these initiatives into their budget cycles, consistent with business needs and missions.

SECTION V – RESPONSIBILITIES

13. The Director, Office of Management and Budget (OMB), within existing authorities of reference c, shall oversee the development of EAs, and the IA integration requirements thereof, in concert with this policy.

14. In coordination, the Secretary of Defense (SECDEF) and the Director of National Intelligence (DNI) shall direct the Director, National Security Agency (DIRNSA) within existing National Manager authorities of reference n, to review the FEA SPP and propose changes to OMB that will ensure proper integration of IA within NSI Components of EA.

15. Federal Government Departments and Agencies shall:

a. Review the FEA Reference Models and their components including, but not limited to, SPPs, Lines of Business (LOBs), service types, functional areas, and performance measures to insure proper integration of IA within NSI Components of EA. Changes to the reference models and their components shall be submitted to OMB in accordance with reference i.

b. Establish responsibilities for control and oversight of IA integration within their EAs.

c. Develop an SPP in accordance with reference l to define IA requirements.

d. Coordinate EA development with all other Departments and Agencies developing such architectures in accordance with references a, f, g, and h.

e. Adhere to the guidance of the Chief Information Officers (CIO) Council, which is responsible through its committees to perform the technical configuration management for the FEA and act as the federated governance mechanism.

f. Establish IA requirements and performance metrics.

g. Develop and coordinate the means to maintain and modernize the IA component of their EAs, including their business, personnel, technical, and security components.

h. Incorporate architecture development topics into IA training, education and awareness, as appropriate.

i. Require an annual review of their existing IA policies to ensure compliance with this policy.

j. Ensure that all acquisitions related to NSI Components of EA comply with this policy.

k. Develop, fund, implement, and manage programs necessary to assure that the goals of this policy are achieved and that plans, programs and CNSS issuances that implement this policy are fully supported.

SECTION VI – (U) QUALIFICATIONS, EXCLUSIONS, AND EXCEPTIONS

16. Subject to policy and guidance for non-NSI Components of EA, Federal Departments and Agencies may wish to consider the requirements of this policy for those EAs which (a) describe the collection, generation, processing, storage, display, or transmission of information that, although not classified, may be critical or essential to the conduct of organizational missions, (b) may be associated with the operation and/or maintenance of critical infrastructures, or (c) would incur prohibitive replacement costs.

17. Nothing in this policy should be interpreted as altering or superseding the existing authorities of the Office of the Director of National Intelligence (ODNI).

Encls:
ANNEX A - References
ANNEX B - Definitions

ANNEX A

REFERENCES

The following documents are referenced in this policy:

a. Public Law 107-347 (PL 107-347), *E-Government Act of 2002*, December 17, 2002.

b. Executive Order 13292 (EO 13292), *Further Amendment of EO 12958, Classified National Security Information*, March 28, 2003.

c. Committee on National Security Systems Instruction No. 4009 (CNSSI No. 4009), *National Information Assurance (IA) Glossary*, revised June 2006.

d. Executive Order 13388 (EO 13388), *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, October 27, 2005.

e. Public Law 108-458 (PL 108-458), *Intelligence Reform and Terrorism Act of 2004*, December 17, 2004.

f. Public Law 104-208 (PL 104-208), *Clinger-Cohen Act of 1996*, January 3, 1996.

g. Office of Management and Budget Memorandum M-03-18, *Implementation Guidance for the E-Government Act of 2002*, August 1, 2003.

h. Office of Management and Budget Transmittal Memorandum No. 4, Circular A-130 (OMB A-130), *Management of Federal Information Resources*, November 28, 2000.

i. *The Federal Enterprise Architecture Reference Model Maintenance Process*, June 2005

j. *The Federal Enterprise Architecture Program EA Assessment Framework 2.0*, December 2005

k. *The Federal Transition Framework Model for Cross Government Initiatives, Release 1.0*, February 2006.

l. *The Federal Enterprise Architecture Security and Privacy Profile*, Version 2.0, May 1, 2006.

m. Title III of the E-Government Act (Public Law 107-347), *Federal Information Security Management Act* (FISMA), December 17, 2002.

n. National Security Directive 42 (NSD 42), *National Policy for the Security of National Security Telecommunications and Information Systems*, July 5, 1990.

ANNEX B

DEFINITIONS

1. *Enterprise Architecture (EA)*: A strategic information asset base that defines the mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs, and includes a baseline architecture, a target architecture, and a sequencing plan.

2. *Federal Enterprise Architecture (FEA)*: A business-based framework developed by the Office of Management and Budget (OMB) for government-wide improvement in developing enterprise architectures by providing a common framework to identify opportunities to simplify processes and unify work across the Federal Government.