Department of Homeland Security
DHS Directives System
National Security Systems Policy Standard Number: 4300B.108-1
Version Number: 9.0
Issue Date: April 19, 2013

National Security System References

I. Purpose

This Standard identifies the foundational references for applying the Risk Management Framework (RMF) to Department of Homeland Security (DHS) National Security Systems (NSS), and establishing an organization-wide risk management program.

II. Scope

This Standard applies to all DHS elements, employees, contractors, detailees, others working on behalf of DHS, and users of DHS NSS that collect, generate, process, store, display, transmit, or receive Confidential, Secret, or Top Secret classified national security information. These NSS include networks, information systems, standalone systems, and applications for which DHS is responsible and has authority, regardless of the physical location.

III. Policy

All Committee on National Security Systems (CNSS) guidance and issuances are considered applicable to NSS. Future revisions of documents identified in this Standard will be reviewed by the DHS OCIO for applicability.

IV. References

A. Below is a foundational listing of legislation and Executive Orders that apply to DHS NSS.

1. Executive Order 12333, *United States Intelligence Activities*, as amended,

December 4, 1981.

2. United States Code, Title 40, Section 11331, “Responsibilities for Federal information systems,” (P.L. 107-217), August 2002.

3. United States Code, Title 44, Subchapter III of Chapter 35, “Federal Information Security Management Act (FISMA) of 2002,” (P.L. 107-347), December 2002.

4. Office of Management and Budget (OMB) Circular No. A-130, Appendix III, “Security of Federal Automated Information Resources,” November 28, 2000.

B. Below is a foundational listing of policies, directives, instructions, regulations, and guidelines that apply to DHS NSS.

5. Committee on National Security Systems (CNSS) Policy Number 22, *Policy on Information Assurance Risk Management for National Security Systems*, January 2012.

6. Committee on National Security Systems (CNSS) Directive 505, *Supply Chain Risk Management*.

7. Committee on National Security Systems (CNSS) Instruction 1001, *National Instruction on Classified Information Spillage*, February 2008.

8. Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security System*, March 2012.

9. Committee on National Security Systems (CNSS) Instruction 4005, *Safeguarding Communications Facilities and Materials*, November 2010.

10. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, April 2010.

11. Committee on National Security Systems (CNSS) Instruction 7003, *Protected Distribution Systems (PDS)*.

12. Department of Homeland Security (DHS) Instruction Manual 121-01-001, *Acquisition Management Instruction/Guidebook*, October 2011.

13. Department of Homeland Security (DHS) Management Directive (MD) 140-01, *Information Technology Systems Security*, July 2007.

14. Department of Homeland Security (DHS) Management Directive (MD)

4400.1, *DHS Web (Internet, Intranet, and Extranet Information) and Information Systems*, March 2003.

15. Department of Homeland Security (DHS) Management Directive (MD) 4500.1, *DHS E-mail Usage*, March 2003.

16. Department of Homeland Security (DHS) Management Directive (MD) 4600.1, *Personal Use of Government Office Equipment*, April 2003.

17. Department of Homeland Security (DHS) Management Directive (MD) 4900, *Individual Use and Operation of DHS Information Systems/Computers*.

18. Department of Homeland Security (DHS) Instruction 121-01-011, *The Department of Homeland Security Administrative Security Program*, April 2011.

19. Department of Homeland Security (DHS) Instruction Handbook 121-01-007, *The Department of Homeland Security Personnel Suitability and Security Program*, June 2009.

20. *DHS Privacy Incident Handling Guidance*, January 2012.

21. Department of Homeland Security (DHS) Sensitive Systems Policy Directive 4300A, Version 9.1, July 2012.

22. Department of Homeland Security (DHS) 4300A Sensitive Systems Handbook, Version 9.1, July 2012.

23. Department of Homeland Security (DHS) 4300B National Security Systems Handbook, Attachment Q, Communication Security (COMSEC), Version 4.0, June 2006.

24. Department of Homeland Security Acquisition Regulation (HSAR), June 2006.

25. Department of Homeland Security (DHS) Privacy Office Guide to Implementing Privacy, Version 1.0, June 2010.

26. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication (Pub) 140-2, *Security Requirements for Cryptographic Modules*, May 2001, to include December 2002 change notices.

27. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

28. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, *Guide to Conducting Risk Assessments*, September 2012.

29. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, November 2010.

30. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework for Federal Information Systems: A Security Life Cycle Approach*, February 2010.

31. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, Revision 1, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

32. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002*.*

33. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, to include May 2010 errata updates.

34. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010.

35. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012.

36. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.

37. National Security Agency/ Central Security Service (NSA/CSS) Policy Manual 9-12, *NSA/CSS Storage Device Declassification Manual.*

38. Standards of Ethical Conduct for Employees of the Executive Branch, September 30, 1999.

C. This is not to be considered an all-inclusive, comprehensive listing. Due to the dynamic nature of NSS, guidance and requirements to protect NSS are constantly evolving, and it is the Information System Owner's and Program Manager's responsibility to maintain awareness of new or updated NSS safeguarding requirements.

V. Responsibilities

Refer to NSS Policy Directive 4300B.100, *Safeguarding and Risk Management for National Security Systems*, Enclosure 2, for organization-wide roles and responsibilities for NSS. For responsibilities specific to steps within the Risk Management Framework (RMF) as applied to DHS, refer to NSS Policy Instruction 4300B.101, *Risk Management Framework for National Security Systems*.