Homeland Security

DHS National Security Systems Policy Directive 4300B

Version 10.1
Issue Date: 11/21/2018

This implements DHS Directive 140-01,
“Information Technology Security Program”

Chip Fulghum
Deputy Under Secretary for Management

11/21/18
Date

This page intentionally left blank.

FOREWARD

The Department of Homeland Security (DHS) 4300 series of information security publications are the official documents that articulate Departmental policies, standards, and guidelines in accordance with DHS Directive 140-01, *Information Technology Security Program*.

Comments concerning DHS National Security Systems (NSS) Information Security publications are welcomed and should be submitted to the DHS Director for the National Security Cyber Division at NSSINFOSEC@hq.dhs.gov or addressed to:

DHS Director for the National Security Cyber Division
OCIO CISO Stop 0182
Department of Homeland Security
245 Murray Lane SW
Washington, D.C. 20528-0182

This page intentionally left blank.

Table of Contents

1.0 Purpose

Adherence to this National Security Systems (NSS) Policy satisfies Federal Cyber Security and Safeguarding Principles for the Department of Homeland Security (DHS).

This Policy provides standardized safeguarding, risk management guidance, and references for use in the management of all DHS NSS Information Technology (IT)[1] equities that are under the purview of the DHS Secretary or DHS Components.

2.0 Scope

This Policy 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 Unclassified, Confidential, Secret, Top Secret, and Special Access Program (SAP) National Security Information (NSI). These NSS include networks, isolated Local Area Networks (LANs), standalone systems, acquisition of IT and/or services, and applications for which DHS is responsible and has authority, regardless of the physical location.

This Policy shall not alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information (SCI) or SCI within a SAP for intelligence as directed by Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended.

This Policy Directive supersedes the DHS National Security Systems Policy Directive 4300B, "*National Security Systems Policy Directive*", Version 10.0, May 2016.

3.0 Authorities

3.1 "Federal Cybersecurity Enhancement Act of 2016"

3.2 DHS Delegation 04000, "Delegation to the Chief Information Officer"

3.3 DHS Directive 140-01, "Information Technology Systems Security"

3.4 DHS Directive 047-01, "Privacy Policy and Compliance"

[1] This Policy shall not alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information (SCI) or SCI within a SAP for intelligence as directed by Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended.

3.5 DHS Directive 140-04, "*Special Access Programs*"

3.6 DHS Instruction 140-04-001, "Special Access Program Management Administration and Oversight"

3.7 National Institute of Standards and Technology, "Cybersecurity Framework", Version 1.1, April 16, 2018

4.0 Definitions

Definitions specific to NSS are defined in Committee on National Security Systems Instruction (CNSSI) 4009, "National Information Assurance Glossary". The terms, as defined in CNSSI 4009, "safeguarding", "information security", and "information assurance" may be used interchangeably throughout this policy. Definitions related to SAPs are defined in DHS MD 140-04 and subordinate instruction(s).

5.0 References

For a listing of references that apply to DHS NSS, refer to Policy Instruction 4300B.108-1, "DHS National Security Systems References".

6.0 Responsibilities

For a listing of responsibilities that apply to DHS NSS, refer to Policy Instruction 4300B.101-1, "DHS National Security Systems Roles and Responsibilities".

7.0 Policy and Requirements

7.1 Policy

7.1.1 DHS shall implement the NSS policies set forth in this document and the 4300B policy series of documents regarding information security through the implementation of risk management programs within the Department.

7.1.2 DHS shall implement CNSS and National Institute of Standards and Technology (NIST) issuances where applicable or as specifically directed in this document or subordinate 4300B issuances. For DHS SAP, safeguarding guidance will be implemented in accordance with the Department of Defense (DoD) "Joint Special Access Program (SAP) Implementation Guide (JSIG)", April 11, 2016.

7.1.3 In accordance with CNSS Policy No. 22, Cybersecurity Risk Management, DHS shall establish and implement an integrated organization-wide program for managing information security risk to DHS NSS in support of organizational operations, assets, or individuals.

7.1.4 DHS organizational elements shall make appropriate assessment and authorization documentation available to other organizations to support the reciprocity and reuse of NSS to the greatest extent possible.

7.2 Requirements

The requirements of the DHS NSS Risk Management and Cybersecurity Frameworks must be integrated and addressed during the full life cycle and implemented as described in DHS 4300B.101. This shall include:

- Identification and inclusion of information security requirements in the design, acquisition, installation, operation, upgrade, or replacement of all DHS NSS. Resources for implementing the NSS RMF within DHS organizational elements shall be identified and allocated as part of planning, programming, and budgeting.

- Inclusion of the NIST, Cybersecurity Framework, into the risk management of NSS.

8.0 Objectives

The Department strives to support, at a minimum, the core program areas listed below:

- Implementing the DHS NSS RMF to evaluate and prioritize risks, determine the appropriate responses to such risks, and enable DHS senior leadership to make informed and timely risk-based decisions;

- Safeguarding, to include Confidentiality, Integrity, and Availability of the system and its information;

- Programs to establish accountability; and

- Programs to ensure that the Department applies life cycle cost analysis methodologies to select the best alternative when making decisions.

9.0 Document Change History

Version	Date	Description
4300B, Version 10.1	November 21, 2018	All references have been updated. A Change Document Page is included in each document of 4300B to reflect the revisions made.
4300B.108-1 Version 10.0	May 4, 2016	Updated all outdated references and added any new references that were applicable to NSS.
4300B.102 Version 10.0	May 2, 2016	Added Privacy controls to reflect latest DHS Privacy guidance.
4300B.102 Version 10.0	May 2, 2016	Updated controls and control enhancements to reflect NIST SP 800-53 r4, CNSSI 1253, and latest DHS NSS Supplemental Guidance.
4300B.101-1 Version 10.0	April 25, 2016	Added the Department NSS Enterprise Information Security Architect.
4300B.101-1 Version 10.0	April 25, 2016	Incorporated the NSS Risk Executive (function).
4300B.101-1 Version 10.0	April 25, 2016	Created DHS Chief Privacy Officer role and the associated responsibilities.
4300B.101-1 Version 10.0	April 25, 2016	Updated all roles and their associated responsibilities as they are in regards to DHS NSS and the DHS RMF.
4300B.101 Version 10.0	May 6, 2016	Added Privacy role to the NSS RMF.
4300B.101 Version 10.0	May 6, 2016	Updated Roles and Responsibilities in the RMF to reflect FISMA 2014.

Version	Date	Description
4300B.100 Version 10.0	May 4, 2016	Added Privacy Directive to authorities section.
4300B.100 Version 10.0	April 4, 2016	Updated all outdated references to reflect latest CNSSI 1253 and NIST SP 800 Rev 4.

10.0 Questions

Address any questions or concerns regarding this Policy to the Director, National Security Cyber (DNSC) Division under the DHS Chief Information Security Officer (CISO).

11.0 Appendix

11.1 4300B Reference Table

4300B.100 *Establishes the 4300B Policy*	**4300B.100** **DHS National Security Systems Policy** *Establishes the DHS policy and requirements regarding the implementation of the Risk Management for National Security Systems (NSS).*
4300B.101 *Implementation Guidance for the RMF*	**4300B.101** **DHS National Security Systems: Risk Management** *Establishes the RMF process for DHS NSS and provides guidance for executing and maintaining the RMF.*
4300B.101-1 *DHS NSS Roles & Responsibilities*	**4300B.101-1** **DHS National Security Systems: Roles and Responsibilities** *Establishes the RMF roles and responsibilities for DHS NSS.*
4300B.102 *DHS NSS Security Controls Catalog*	**4300B.102** **DHS National Security Systems: Control Guidance** *Provides the DHS requirements regarding implementation of the security controls with both Committee on National Security Systems (CNSS) and DHS defined values, for all NSS.*
4300B.103 *Templates provided for standardized guidance and format for DHS NSS*	**4300B.103-1** **Template for System Security Plans** **4300B.103-2** **Template for Risk Assessment Reports** **4300B.103-3** **Template for Security Assessment Reports** **4300B.103-4** **Template for Plan of Action and Milestones**
4300B.104	**4300B.104** **DHS NSS Continuous Monitoring – TBD**
4300B.105	**4300B.105**

	DHS NSS Cross Domain Solutions – TBD
4300B.106 *General and Privileged User Rules of Access and Behavior*	**4300B.106** **DHS NSS General and Privileged User Account Access Request Minimum Requirements** *Providing guidance and minimum requirements for General and Privileged User Account Request agreements.*
4300B.107 *Guidance when a DHS NSS is to be removed from service*	**4300B.107** **DHS NSS Decommissioning Strategy Minimum Requirements** *Minimum requirements for a standardized, systematic approach for decommissioning NSSs.*
4300B.108	**4300B.108-1** **DHS National Security Systems: References** **4300B.108-2** **DHS National Security Systems: Policy Change Request**