Homeland Security

U.S. Department of Homeland Security

DHS 4300A, "Sensitive Systems"

Attachment W

ROLES AND RESPONSIBILITIES

Version 1.0

April 28, 2022

Document Change History

Version	Date	Description
1.0	April 28, 2022	Processes and authorities updated by Jeremy Tucker, Division Chief, Engineering, ITO

4.1.2 Component CISOs:

Serve as principal advisor on information security matters. The Component CISO implements and manages all aspects of the Component Information Security Program to ensure compliance with DHS policy and guidance implementing FISMA, other laws, and Executive Orders. The Component CISO reports directly to the Component CIO on matters relating to the security of Component information systems.

4.1.3 Component Information Systems Security Manager (ISSM)

Components that are not required to have a fulltime CISO must have a fulltime Information Systems Security Manager (ISSM). The ISSM is designated in writing by the Component CIO, with the concurrence of the DHS CISO.

4.1.4 Risk Executive

A Risk Executive ensures that risks are managed consistently across the organization. In keeping with its organizational structure, DHS has two levels of Risk Executive: Departmental and Component.

4.1.5 Authorizing Official (AO)

The AO formally assumes responsibility for operating an information system at an acceptable level of risk. The AO assigns the Security Control Assessor for the system.

4.1.6 Security Control Assessor

The Security Control Assessor is a senior management official whose responsibilities include certifying the results of the security control assessment. A Security Control Assessor is assigned in writing to each information system by the Component CISO.

4.1.7 Information Systems Security Officer (ISSO)

An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO.

4.1.8 Ongoing Authorization (OA) Manager and Operational Risk Management Board (ORMB)

Each Component has an OA Manager responsible for evaluating and tracking security events for systems operating under the DHS OA Program. Component OA Managers:

4.1.9 DHS Security Operations Center (SOC)

The DHS Enterprise SOC (DHS SOC) is charged to act as a single point for DHS enterprise-wide cyber situational awareness. As such, DHS Enterprise SOC provides incident management oversight for all incidents detected and reported from all sources.

4.1.10 Component Security Operations Centers

Component SOCs are responsible for incident response, handling and reporting those incidents that pertain to the Component's network and data.

5. Ensures that information security processes are integrated with strategic and operational planning processes to secure the Department's mission
6. Ensures that the Department's senior officials have the necessary authority to secure the operations and assts under their control
7. Delegates authority to the USM, who delegates to the OCIO to ensure compliance with applicable information security requirements

5.1.1 DHS Chief Information Officer

The DHS Chief Information Officer (CIO) is the senior agency executive responsible for all DHS information systems and their security as well as for ensuring FISMA compliance.

The responsibilities of the DHS CIO include:

1. Develops and maintains the DHS Cybersecurity program.
2. Designates the DHS CISO.
3. Approves all interconnections between DHS enterprise-level information systems and non-DHS information systems. The DHS CIO ensures that connections with other Federal Government agencies are properly documented. A single ISA may be used for multiple connections provided that the security authorization is the same for all connections covered by that ISA.
4. May revoke the ATO of any DHS information system.
5. Provides guidance, direction, and authority for a standard DHS-wide process for contingency planning for information systems.
6. Heads the office with the mission and resources to assist in ensuring Component compliance with the DHS Information Security Program.
7. Oversees the development and maintenance of a department-wide information security program.
8. Issues Department-wide information security policy, guidance, and architecture requirements for all DHS systems, networks, and IS-related supply chains. Security policies incorporate National Institute of Standards and Technology (NIST) guidance, as well as all applicable OMB memorandums and circulars.
9. Appoints in writing a DHS employee to serve as the DHS CISO.
10. As appropriate, serves as or appoints in writing the AO for DHS enterprise information systems.

11. Ensures the development of DHS performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the Department-wide security program.
12. Ensures that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies.
13. Ensures that DHS security programs integrate fully into the DHS enterprise architecture and capital planning and investment control processes.
14. Ensures that System Owners understand and appropriately address risks, including supply chain risk and risks arising from interconnectivity with other programs and systems outside their control.
15. Reviews and evaluates the DHS Information Security Program annually.
16. Ensures that an information security performance metrics program is developed, implemented, and funded.
17. Reports to the DHS Under Secretary for Management on matters relating to the security of DHS systems.
18. Ensures compliance with applicable information security requirements.
19. Implements firewall changes as requested by DHS and Component CISOs.
20. Coordinates and advocates resources for enterprise security solutions.
21. Leads the DHS Information Systems Contingency Planning program.

5.1.2 Component Chief Information Officer

The Component CIO is responsible for Component information systems and their security as well as for ensuring FISMA compliance within the Component.

The responsibilities of the Component CIO include:

1. Develops and maintains the Component Information Security Program.
2. May revoke the ATO of any Component-level information system.
3. Establishes and oversees their Component information security programs
4. Directs a review of the Component information security program plan be performed with a frequency depending on risk, but no less than annually.
5. Ensures that an AO has been appointed for every Component information system; serves as the AO for any information system for which no AO has been appointed or where a vacancy exists.

6. Ensures that information security concerns are addressed by Component Configuration Control Boards, Enterprise Architecture Board (EAB), Acquisition Review Board (ARB), and Investment Review Board (IRB).
7. Ensures that an accurate information systems inventory is established and maintained.
8. Ensures that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies.
9. Ensure that System Owners understand and appropriately address risks, including supply chain risk and risks arising from interconnectivity with other programs and systems outside their control.
10. Ensures that an information security performance metrics program is developed, implemented, and funded.
11. Advises the DHS CIO of any issues regarding infrastructure protection, vulnerabilities or the possibility of public concern.
12. Ensures that incidents are reported to the DHS ESOC within the timeframes defined in Attachment F, "Incident Response" of the DHS 4300A Sensitive Systems Handbook.
13. Works with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.
14. Ensures compliance with DHS information systems security policy.
15. Coordinates and advocate resources for information security enterprise solutions.
16. CIOs of the CBP, FEMA, FLETC, ICE, TSA, USCIS, USCG, and USSS appoint a CISO that reports directly to the Component CIO and ensure that the CISO has resources to assist with Component compliance with policy.
17. CIOs of all other Components:
    a. Ensures that Component ISSMs have been appointed.
    b. Provides the resources and qualified personnel to ensure Component compliance with DHS security policy.

5.1.3 DHS Chief Information Security Officer

The DHS CISO implements and manages the DHS Information Security Program to ensure compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations.

The DHS CISO reports directly to the DHS Chief Information Officer (CIO) and is the principal advisor on information security matters.

The responsibilities of the DHS CISO include:

1. Serves as the CIO's primary liaison with the organization's Authorizing Officials (AO), information System Owners (SO) and Information Systems Security Officers (ISSO).
2. Represents DHS on the Federal PKI Policy Authority (FPKIPA).
3. Conducts information security reviews and assistance visits across the Department in order to monitor the effectiveness of Component security programs.
4. Reviews information security policies submitted by Components.
5. Maintains a repository for all Security Authorization Process documentation and modifications.
6. Specifies tools, techniques, and methodologies used to assess and authorize DHS information systems, report, and manage Federal Information Security Modernization Act of 2014 (FISMA) data, and document and maintain POA&Ms.
7. Ensures preparation and maintenance of plans and procedures to provide continuity of operations for information systems.
8. Issues department-wide information security policy, guidance, and information security architecture requirements for all DHS systems.
9. Implements and manages the Department-wide Information Security Program and ensures compliance with the FISMA, Office of Management and Budget (OMB) directives, and other Federal requirements.
10. Facilitates development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems.
11. Serves as the principal Departmental liaison with organizations outside DHS in matters relating to information security.
12. Establishes and institutionalizes contact with selected groups and associations within the security community:
    i. To facilitate ongoing security education and training for organizational personnel;
    ii. To maintain currency with recommended security practices, techniques, and technologies; and
    iii. To share current security-related information including threats, vulnerabilities, and incidents.
13. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: (1) are developed and maintained; and (2) continue to be executed in a timeline

manner.

14. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
15. Implements a threat awareness program that includes a cross-organization information-sharing capability.
16. Reviews and approves the tools, techniques, and methodologies planned for use in certifying and authorizing DHS systems, and for reporting and managing systems- level FISMA data. This responsibility includes reviews and approval of Security Control Assessment plans, Contingency Plans, and security risk assessments.
17. Consults with the DHS Chief Security Officer (CSO) on matters pertaining to physical security, personnel security, information security, investigations, and Sensitive Compartmented Information (SCI) and Special Access Program (SAP) systems, as they relate to information security and infrastructure.
18. Develops and implements procedures for detecting, reporting, and responding to information security incidents.
19. Chairs the CISO Council. The Council is composed of all Component CISOs, and is the Department's primary coordination body for any issues associated with information security policy, management, and operations. Component CISOs and Information Systems Security Managers (ISSM) will be invited to CISO Council meetings as required.
20. Maintains a comprehensive inventory of all general support systems (GSS) and major applications (MA) in use within the Department:

    i. Security management for every GSS is under the direct oversight of either the DHS CISO (for enterprise systems) or a Component CISO/ISSM (for Component-specific GSSs).

    ii. MAs are under the direct control of either a Component CISO or Component ISSM.
21. Maintains a repository for all Information Assurance (IA) security authorization process documentation and modifications.
22. Performs security reviews for all planned information systems acquisitions over $2.5 million and for additional selected cases.
23. Provides oversight of all security operations functions within the Department.
24. Maintains classified threat assessment capability in support of security operations.
25. Performs annual program assessments for each of the Components.

26. Performs periodic compliance reviews for selected systems and applications
27. Publishes monthly Compliance Scorecards.
28. Delegates specific responsibilities and assigns responsibilities to Component CISOs and ISSMs as appropriate for maintaining a high degree of compliance.
29. As required by DHS Directive 140-01, reports annually, through the CIO and USM, to the Secretary on the effectiveness of the Department information security program, including progress of remedial actions. The CISO's annual report provides the primary basis for the Secretary's annual report to both OMB and to the United States Congress that is required by FISMA.
30. Assists senior Department officials concerning their responsibilities under FISMA.
31. Heads an office with the mission and resources to assist in ensuring Department compliance with information security requirements.
32. Appoints a DHS employee to serve as the Headquarters CISO.
33. Appoints a DHS employee to serve as the Office of Intelligence and Analysis (I&A) CISO.
34. Provides operational direction to the DHS Enterprise Security Operations Center (ESOC).

5.1.4 Component Chief Information Security Officer

The Component Chief Information Security Officer (CISO) implements and manages all aspects of the Component Information Security Program to ensure compliance with DHS policy and guidance implementing FISMA, other laws, and Executive Orders. The Component CISO reports directly to the Component CIO on matters relating to the security of Component information systems. In order to ensure continuity of operations and effective devolution, large Components should ensure the designation of a Deputy CISO with full authorities, to include the roles of Risk Executive and Security Control Assessor (upon the absence of the CISO).

The responsibilities of the Component CISO include:

1. Develop and maintain a Component-wide information security program in accordance with the DHS security program.
2. All Components are accountable to the Component CISO for the information security program. Components without a fulltime CISO are responsible to the DHS CISO.
3. Establish and enforce Component-level malware protection control policies.
4. Responsible for management oversight of the DHS PCA RA activities and personnel within the Component.

i. The DHS Federal Public Key Infrastructure (FPKI) is governed by the U.S. Common Policy Framework certificate policy approved by the FPKIPA, and by the relevant portions of the Department of the Treasury Infrastructure (PKI) X.509 Certificate Policy approved by the Department of the Treasury Policy Management Authority (PMA).

ii. The DHS Internal Use NPE PKIs are governed by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines approved by the DHS PKIPA.

5. Coordinate with the relevant Component Security Operations Center (SOC) and DHS SOC when vulnerability assessment responsibilities encompass more than one Component.
6. Approve and manage all activities relating to Vulnerability Assessment Team (VAT) to support incidents, internal and external assessments, and on-going SELC support.
7. Acknowledge receipt of Information Security Vulnerability Management (ISVM) messages.
8. Provide emergency and temporary access authorization and approval.
9. Ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of information systems and that security-related decisions and information are distributed to the ISSOs and other stakeholders.
10. Review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO annually.
11. Establish usage restrictions and implementation guidance for wireless technologies.
12. Authorize, monitor, and control wireless access to DHS information systems.
13. Ensure that weekly incident response tracking is performed for all of their perspective CFO-designated systems.
14. Ensure that vulnerability assessments and verification of critical path installations are conducted on all CFO-designated systems, at least annually.
15. Report all types of privacy incidents, whether or not they involve information resources for Components without Privacy Officers or PPOCs. This unitary reporting process remains in effect until each Component has a Privacy Officer or PPOC who can fulfill the reporting duties.
16. Establish processes to ensure that the Security Authorization Process is used consistently for all Component systems.
17. Ensure that a risk assessment is conducted whenever modifications are made to sensitive information systems, networks, or their physical environments, interfaces, or user community. All Security Plans are updated and systems are re-authorized, if required.

18. Ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.
19. Ensure that a risk assessment is conducted when major modifications that have the potential to significantly impact risk are made to sensitive information systems, or to their physical environments, interfaces, or user community. The risk assessment considers the effects of the modifications on the operational risk profile of the information system. SPs are updated and re-certifications conducted, if required, by the results of the risk assessment.
20. Establish an independent Component-wide Security Authorization program to ensure a consistent approach to testing the effectiveness of controls.
21. Ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.
22. Ensure that all Continuity of Operations (COOPs), under their purview, are tested and exercised annually.
23. Implement DHS information security policies, procedures, and control techniques to meet all applicable requirements.
24. Develop and manage information security guidance and procedures unique to Component requirements.
25. Ensure that information systems comply with the DHS Enterprise Architecture (EA) Technical Reference Model (TRM) and Security Architecture (SA) or, for deviations, maintain a waiver approved by the DHS CIO or CISO.
26. Submit information security reports regarding DHS systems to the Senior Component official or designee.
27. Serves as principal advisor on information security matters.
28. Reports directly to the Component CIO on matters relating to the security of Component information systems.
29. Oversees the Component information security program.
30. Ensures that information security-related decisions and information, including updates to the 4300 series of information security publications, are distributed to the ISSOs and other appropriate persons within their Component.
31. Approves and/or validates all Component information system security reporting.
32. Consults with the Component Privacy Officer or Privacy Point of Contact (PPOC) for reporting and handling of privacy incidents.

33. Manages information security resources including oversight and review of security requirements in funding documents.
34. Review and approve the security of hardware and software prior to implementation into the Component SOC.
35. Provide operational direction to the Component SOC.
36. Periodically test the security of implemented systems.
37. Implement and manage a Plan of Action and Milestones (POA&M) process for remediation by creating a POA&M for each known vulnerability.
38. Ensure that ISSOs are appointed for each information system managed at the Component level, and review and approve ISSO appointments.
39. Ensure that weekly incident reports are submitted to the DHS ESOC.
40. Acknowledge receipt of Information System Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers.
41. Manage Component firewall rule sets.
42. Ensure that Interconnection Security Agreements (ISA) are maintained for all connections between systems that do not have the same security policy.
43. Ensure adherence to the DHS Secure Baseline Configuration Guides
44. Ensure reporting of vulnerability scanning activities to the DHS ESOC, in accordance with DHS 4300A Information Technology Security Program Sensitive Systems Attachment O, "Vulnerability Management Program."
45. Develop and maintain a Component-wide information security program in accordance with Department policies and guidance.
46. Implement Department information security policies, procedures, and control techniques to ensure that all applicable requirements are met.
47. Ensures general awareness and role-based training and oversight for all Component personnel especially those with significant responsibilities for information security.
48. Oversee the Component's Security Authorization process for GSSs and MAs.
49. Maintain an independent Component-wide assessment program to ensure that there is a consistent approach to controls effectiveness testing.
50. Ensure that an appropriate SOC performs an independent network assessment as part of the assessment process for each authorized application.
51. Ensure that enterprise security tools are utilized.
52. Oversee all Component security operations functions, including the Component SOCs.

53. Ensure that external providers who operate information systems on behalf of the Component meet the same security requirements as required for government information and information systems.
54. Ensure an acceptable level of trust for each external service, either by accepting risk or by using compensating controls to reduce risk to an acceptable level.
55. Ensure that systems engineering lifecycle activities implement processes that include software assurance and supply chain risk management.
56. Issue a Component Supply Chain Risk Management (SCRM) Plan that defines how Component programs and systems develop and execute their individual SCRM plans or adopt SCRM into Security Plans.
57. Serves as the Security Control Assessor (SCA), if required.

5.1.5 Heads of DHS Components

The Heads of DHS Components are responsible for oversight of their Components' information security program, including the appointment of CIOs, subject to the approval of the DHS CIO. Heads of Components allocate adequate resources to information systems for information system security.

The responsibilities of Heads of DHS Components include:

1. Ensures that information systems and their data are sufficiently protected.
2. Appoints CIOs, subject to the approval of the DHS CIO.
3. Ensures that an Information Security Program is established and managed in accordance with DHS policy and implementation directives.
4. Ensure that the security of information systems is an integral part of the life cycle management process for all information systems developed and maintained within their Components.
5. Ensure that adequate funding for information security is provided for Component information systems and that adequate funding requirements are included for all information systems budgets.
6. Ensure that information system data are entered into the appropriate DHS Security Management Tools to support DHS information security oversight and FISMA reporting requirements.
7. Ensure that the requirements for an information security performance metrics program are implemented and the resulting data maintained and reported.

5.1.6 Risk Executive

A Risk Executive ensures that risks are managed consistently across the organization. In keeping with its organizational structure, DHS has two levels of Risk Executive: Departmental and Component. The risk executive provides a holistic view of risk beyond that associated with the operation and use of individual information systems. Risk Executive observations and analyses are documented and become part of the security authorization decision.

The responsibilities of a Risk Executive include:

1. Ensure that management of security risks related to information systems is consistent throughout the organization, reflects organizational risk tolerance, and is performed as part of an organization-wide process that considers other organizational risks affecting mission and business success.
2. Ensure that information security considerations for individual information systems, including the specific authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization.
3. Ensures that information security considerations for individual information systems, including the specific authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization.
4. Provides visibility into the decision of AOs and a holistic view of risk to the organization beyond the risk associated with the operation and use of individual information systems, including those associated with the supply chain.
5. Facilitates the sharing of security-related and risk-related information among AOs and other senior leaders in the organization in order to help those officials consider all types of risks that could affect mission and business successes and the overall interests of the organization at large.
6. Ensures that System Owners, ISSOs, and AOs monitor and manage supply chain risks, as part of the overall Component risk management strategy.
7. Develops information security policy, establishes the standards for system security risk, oversees risk management and monitoring, and approves all waivers to DHS policy.
8. Component Risk Executives may establish system security risk standards more stringent than DHS standards. Risk Executives implement the system security risk management and monitoring program and submit requests for higher-risk deviations from the enterprise standard.
9. The DHS CIO is the DHS Risk Executive. The DHS CIO has delegated this authority to

the DHS CISO.

10. Each Component CIO is the Risk Executive for his or her Component. The Component CIO may delegate this authority to the Component CISO.
11. The Risk Executive performs duties in accordance with NIST SP 800-37.
12. Risk Executives review recommendations for risk determinations and risk acceptability and may recommend changes to the AO and appropriate CIO.

5.1.7 Authorizing Official

The Authorizing Official (AO) formally assumes responsibility for operating an information system at an acceptable level of risk. The AO is a senior management official and a Federal employee.

The responsibilities of the AO include:

1. Assigns the SCA for the system.
2. The DHS CIO acts as the AO for enterprise information systems, excluding financial systems, or designates an AO in writing for DHS mission systems and for multi-Component systems without a designated AO.
3. The DHS CIO acts as the AO for enterprise information systems, excluding financial systems, or designates an AO in writing for DHS mission systems and for multi-Component systems without a designated AO.
4. The Component CIO acts as the AO for Component information systems, excluding financial systems, or designates an AO in writing for all systems without a designated AO.
5. Every system has a designated AO. (An AO may be responsible for more than one system.)
6. The AO is responsible for review and approval of any individual requiring administrator privileges. The AO may delegate the performance of this duty to the appropriate System Owner or Program Manager.
7. The AO is responsible for acceptance of remaining risk to organizational operates and assets, individuals, other organizations, and the Nation.
8. The AO periodically reviews security status for all systems under his or her purview to determine if risk remains acceptable.
9. The AO performs additional duties in accordance with NIST SP 800-37.
10. The AO approves appropriate coast-effective countermeasures against denial-of-service

attacks prior to wireless device operation.

11. The AO approves the use of wireless mobile devices or software applications used to process, store, or transmit sensitive information from the NSA Commercial Solutions for Classified (CSFC) Program components list; FIPS 201 Approved Products List (APL); or the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) product list. Mobile devices approved by the AO are posted in the DHS Enterprise Architecture (EA) Approved Products List (APL) of the Technical Reference Model (TRM).
12. The AO formally assumes responsibility for operating an information system at an acceptable level of risk. Operating any system with sensitive information is prohibited without an ATO.
13. The AO for a system is identified in CSAM. The Component CIO serves as the AO whenever the System Owner or an appropriate program official has not been named as the AO.

5.1.8 Information Systems Security Manager

An ISSM serves as the liaison and primary point of contact and coordination between program personnel responsible for cybersecurity activities, assigned ISSOs and the applicable CISO for cybersecurity matters. ISSMs shall be designed in writing by the Component CISO.

The responsibilities of the ISSM include:

1. Serves as the principal interface between the DHS CISO, ISSOs, and other security practitioners.
2. Works directly with the DHS CISO.
3. Establishes and enforces Component-level malware protection control policies.
4. Responsible for management oversight of the DHS PCA RA activities and personnel within the Component.
5. Coordinates with the DHS ESOC and relevant Component SOCs, when vulnerability assessment responsibilities encompass more than one Component.
6. Approves and manages all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and ongoing SELC support.
7. Acknowledges receipt of ISVM messages.

8. Provides emergency and temporary access authorization, if needed.
9. Ensures that weekly incident response tracking is performed for all respective CFO-designated systems.
10. Ensures that annual vulnerability assessments and verification of critical patch installations are conducted on all CFO-designated systems.
11. Reports all types of privacy incidents, if needed.
12. Ensures that risk assessments are conducted when modifications are made to sensitive information systems, networks, physical environments, interfaces, or user community; all supporting documentation are updated accordingly (i.e., SPs) and systems are re-authorized, if required.
13. Ensures that risk assessments are conducted when major modifications, that have potential to significantly impact risk are made to sensitive information systems, physical environments, interfaces, or user community.

    i. The risk assessment considers the effects of the modifications on the operational risk profile of the information system. SPs are updated and re-certifications conducted, if required, based on the results of the risk assessment.
14. Establishes an independent Component-wide Security Authorization program to ensure a consistent approach to testing the effectiveness of controls.
15. Ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.
16. Ensures that all COOPs under their purview are tested and exercised annually.
17. Ensures that their information systems comply with the DHS Enterprise Architecture (EA) Technical Reference Model (TRM) and security architecture (SA), or for deviations, maintain a waiver approved by the DHS CIO or CISO.
18. Oversees the Component information security program.
19. Ensures that the DHS CISO and Component CIO are kept informed of all matters pertaining to the security of information systems.
20. Ensure that all communications and publications pertaining to information security, including updates to the 4300 Policies and Handbooks, are distributed to the ISSOs and other appropriate persons within their Component.
21. Validate all Component information system security reporting.
22. Consult with the Component Privacy Officer or PPOC for reporting and handling of

privacy incidents.

23. Manage information security resources including oversight and review of security requirements in funding documents.
24. Test the security of the Component's information systems periodically.
25. Implement and manage a POA&M process for remediation by creating a POA&M for each known vulnerability.
26. Ensure that ISSOs are appointed for each Component-managed information system.
27. Ensure that weekly incident reports are forwarded to the DHS CISO.
28. Acknowledge receipt of ISVM messages, report compliance with requirements, or notify applicants of the granting of waivers.
29. Ensure adherence to the DHS Secure Baseline Configuration Guides.
30. Develop and publish procedures for implementation of DHS information security policy within the Component.
31. Implement Department information security policies, procedures, and control techniques to address all applicable requirements.
32. Ensure training and oversight for personnel with significant responsibilities for information security.
33. Oversee the Security Authorization process for the Component's MAs.
34. Maintain an independent Component-wide security control assessment program to ensure a consistent approach to controls effectiveness testing.
35. Ensure that an appropriate SOC performs an independent network assessment as part of the security control assessment process for each authorized application.
36. Ensure that enterprise security tools are used.
37. Ensure that ISSOs monitor and manage the information security aspects of supply chain risks. Ensure that ISSOs adopt software assurance principles and tools.

5.1.9 Information Systems Security Officer

An Information Systems Security Officer (ISSO) performs security actions for an information system. Only one ISSO is assigned to a system and multiple Alternate ISSOs may be designated to assist the ISSO. While the ISSO performs security functions, responsibility for information system security always rests with the System Owner.

The responsibilities of the ISSO include:

1. Serves as the Point of Contact (POC) for all security matters related to the designated system.

2. Ensures the implementation and maintenance of security controls in accordance with the Security Plan and DHS policies.
3. ISSOs are federal or contractor employees whose background investigations have been completed in accordance with DHS policy.
4. ISSO duties are not assigned as collateral duties unless approved by the Component CISO.
5. ISSOs have a clearance and access greater than or equal to the highest level of information contained on the system. It is strongly encouraged that ISSOs be cleared to the Secret level in order to facilitate intelligence sharing among information security professionals.
6. Ensures that timely responses are provided to Infrastructure Change Control Board (ICCB) change request packages.

5.1.10 Security Control Assessor

The Security Control Assessor (SCA) is a senior management official whose responsibilities include certifying the results of the security control assessment. A SCA is assigned in writing to each information system by the Component CISO. The SCA and the team conducting a certification are impartial. They are to be free from any perceived or actual conflicts of interest with respect to the development, operational, and or management chains of command associated with the information system, or with respect to the determination of security control effectiveness.

For systems with a low impact, a SCA and/or certifying team does not need to be independent so long as assessment results are carefully reviewed and analyzed by an independent team of experts to validate their completeness, consistency, and truthfulness. The AO decides the required level of assessor independence based on: (1) the criticality and sensitivity of the information system, (2) the ultimate risk to organizational operations, organizational assets, and individuals, and (3) the level of assessor independence required for confidence that the assessment results are sound and valid for making credible risk-based decisions.

The responsibilities of a SCA include:

1. May be responsible for more than one system.
2. May take the lead for any or all remedial actions.
3. Provides an assessment of the severity of weakness or deficiencies in the information systems and prepares the final security control assessment report containing the results and findings from the assessment but not making a risk determination.

5.1.11 DHS Information System Owners

Information System Owners (ISOs) use Information Technology (IT) to help achieve the mission needs within their program area of responsibility. They are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security. For proper administration of security, a System Owner is designated in writing for each system by the AO.

The responsibilities of an ISO include:

1. Ensures that each of their systems is deployed and operated in accordance with this policy document.
2. Ensures that an ISSO is designated in writing for each information system under their purview.
3. There is only one System Owner designated for each DHS system.
4. Ensures information security compliance, development and maintenance of security plans, user security training, notifying officials of the need for security authorization and need to resource.
5. Ensures development of a POA&M to address weaknesses and deficiencies in the information system and its operating environment.
6. The DHS CIO designates a System Owner in writing for DHS mission systems and for multi-Component systems.
7. The Component CIO designates an AO in writing for Component systems.
8. Where systems or programs provide common controls, the System Owners ensure that a security control assessment is completed in the Information
9. Where systems or programs provide common controls, the System Owners ensure that a security control assessment is completed
10. Ensures that risk management activities include addressing supply chain risks for the system's current and all subsequent lifecycle phases and documenting this activity in the SCRM Plan.
11. Ensures that any hardware or software develops a full lifecycle plan based on the vendor's established life expectancy of the product and total cost of ownership. Any new or existing product that will reach end-of-life (EOL)* within three (3) years and is part of a Component IT System will require development of a remediation, upgrade, replacement and funding plan to remove the EOL item(s) from the Component's environment completely within that time frame. A plan of action and milestone shall be submitted for risk acceptance to the Component CISO and AO in order to track remediation milestones appropriately. End of Life (EOL) is defined as production and/or development, technical support, spare parts and security patches which are no longer available from the vendor.
12. Reports the security alert and advisory status of the information system to the AO, Component CISO/ISSM, and DHS CISO upon request and on a periodic basis.
13. Ensures that Contingency plans are created for all CFO Designated Systems requiring moderate availability and that Disaster Recovery Plans are created for all CFO-

designated systems requiring high availability and that each plan is tested annually, and results with lessons learned annually.

14. Use the POA&M process to document the control deficiencies or vulnerabilities, and use the plans to correct the deficiencies and vulnerabilities. The scheduled completion date for system POA&Ms is within one year of POA&M creation and within 6 months for CFO designated systems and high value assets (HVAs).

15. Requests a waiver for information systems that use operating systems or applications that are not hardened or do not follow configuration guidance identified in the DHS Secure Baseline Configuration Guides included in the DHS 4300A Sensitive Systems Handbook. Requests include a proposed alternative secure configuration.

16. Responsible for developing and documenting information system Contingency Plans (CPs) for their information systems, managing plan changes, and distributing copies of the plan to key contingency personnel. Component CIOs review and approve Component-level information system CPs.

17. Includes information security requirements in their CPIC business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS system.

18. Ensures that information security requirements and Plans of Action and Milestones (POA&M) are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.

5.1.12 DHS Enterprise Security Operations Center

The DHS Enterprise Security Operations Center (ESOC) is charged to act as a single point for DHS enterprise-wide cyber situational awareness. As such, the DHS ESOC provides incident management oversight for all incidents detected and reported from all sources. The DHS ESOC also provides the first line of active defense against all cyber threats by monitoring all perimeter network gateways. Lastly, the DHS ESOC oversees the department-wide vulnerability management program.

The responsibilities of the DHS ESOC include:

1. Reviews all reported incidents and verify that all pertinent information is recorded, confirmed, and that closure occurs only after all remediation and reporting activities have occurred in accordance with this Policy Directive.

2. Focuses 24x7 monitoring efforts on shared DHS infrastructure such as the Trusted Internet Connection (TIC), Policy Enforcement Points (PEP), Email Security Gateway (EMSG), Demilitarized Zones (DMZ), Virtual Private Networks (VPN) and other devices as required by DHS CISOs to identify security events of interest that require confirmation, escalation, or declaration as false positive.

3. Creates Security Event Notifications (SEN) based on monitoring and analysis activities when events of interest are identified that require further investigation.

4. Provides oversight on investigational activities and review SENs prior to escalation. SENs will be escalated when Components have sufficiently demonstrated that adequate

investigation has been performed and that the event is a verified incident. The Component provides necessary information regarding the event in accordance with the escalation criteria outlined in Appendix F3, "Response Guidelines".

5. Reviews all SENs for closure and close SENs after all reasonable investigational activities have been completed.
6. Conducts operations and maintenance and approve changes on all security monitoring devices associated with shared DHS infrastructure (such as Intrusion Detection System (IDS), Data Loss Prevention (DLP).
7. Provides oversight and guidance for all incidents to ensure adherence to DHS Sensitive Systems Policy Directive 4300A.
8. Serves as the primary clearinghouse and collection point for information related to incidents involving DHS systems or networks.
9. Coordinates privacy and security incident handling activities with DHS entities such as the DHS Office of Security and the DHS Privacy Office.
10. Ensures that remediation and all necessary coordination activities are completed before incident closure.
11. Analyzes incidents, identifying and notifying other stakeholders and DHS Components and Data Center SOCs that may be affected.
12. Provides technical and investigative assistance to Components and Data Center SOCS as needed.
13. Provides accurate and timely reports to the DHS CISO on significant incidents and on the status of DHS enterprise computer security.
14. Develops and maintains an incident database that contains information on all discovered and reported incidents.
15. Provides automated incident notification and reporting to senior DHS and Component leadership and stakeholders such as the DHS Privacy Office and the DHS Office of Security, as well as external reporting entities such as the United States Computer Emergency Readiness Team (US-CERT).
16. Updates US-CERT on incident status as required.
17. Facilitates communications between DHS Components and Data Center SOCS (when applicable) for those incidents involving more than one Component (i.e., Master incidents).
18. Provides ad hoc incident trending reports as requested by the DHS CISO.
19. Administers and monitors DHS intrusion detection system (IDS) sensors and security devices.
20. All Department and Component firewalls and PEPs are administered in coordination with DHS security operation capabilities, through the DHS ESOC or Component SOC.
21. Reports all operational information to the DHS CISO.

5.1.13 DHS Component Security Operations Centers

The DHS Component SOCs have functional, advisory, and reporting responsibilities in incident response that include the following: focus security monitoring efforts on the Component network and compile and maintain a list of mission-critical systems, financial systems, and applications. The list assists in determining the classification of the Component's systems, and in prioritization of security incidents.

The responsibilities of DHS Component SOCs include:

1. Develops and publish internal computer security incident response plans and incident handling procedures, with copies provided to the DHS ESOC upon request.
2. Investigates SENS and Incidents created by the DHS EESOC and comply with reporting timelines and escalation criteria outlined in DHS 4300A Information Technology Security Program Sensitive Systems Attachment F, "Incident Response," Appendix F3, "Response Guidelines" to either escalate the SEN or close it.
3. Monitors internal network enclave traffic such as firewall logs and Network IDS) and host-based security events (e.g. audit logs and Host-based Intrusion Prevention Systems (IPS) and IDS). This includes workstation activity, internal server enclaves, Component-managed externally accessible applications and networks (e.g. DMZ, VPN), and applications hosted by third parties external to DHS.
4. Requests SEN escalation by the DHS ESOC, within the reporting timeframes and meeting the escalation criteria outlined in DHS 4300A Information Technology Security Program Sensitive Systems Attachment F, "Incident Response," Appendix F3, "Response Guidelines."
5. Conducts SEN and incident investigation including traceback to the host.
6. Requests closure when a SEN has been identified as inconclusive or as a false positive after providing adequate explanation of investigational activities via the Enterprise Operations Center Portal (EOConline).
7. Responds to DHS ESOC on SEN investigation activities based on the escalation criteria in DHS 4300A Information Technology Security Program Sensitive Systems Attachment F, "Incident Response," Appendix F3, "Response Guidelines."
8. Ensures 24x7 incident handling function exists for the Component.
9. Leads the Component's incident handling and response activities, including identification, investigation, containment, eradication, and recovery. Coordinate incident response, investigation, and reporting to the DHS ESOC. Reporting should include all significant data, such as the who, what, when, where, why, and how of a given incident. Coordinate incident handling activities with internal Component entities such as the Component Office of Security, Component Privacy Office, and Internal Affairs.
10. Coordinates Component-level remediation efforts as mandated by DHS security policies and communicate remediation activity to DHS ESOC through EOConline log entries.
11. Shares applicable information Department-wide or Component-wide, for example by providing network and host-based indicators for malicious logic incidents; such indicators facilitate implementation of proactive measures to prevent future incidents.

12. Provides updates to the DHS ESOC for significant incidents whenever additional information becomes available.
13. Requests closure of incidents when Component remediation and mitigation actions have concluded.
14. Assists other Components with technical or investigation assistance as requested by the DHS ESOC.
15. Utilizes security automation tools and technologies that facilitate efficient machine and human data exchange with the DHS ESOC, with the National Cybersecurity and Communications Integration Center (NCCIC), and with peer SOCs to the maximum extent possible.

5.1.14 DHS Chief Security Officer

The DHS Chief Security Officer (CSO) implements and manages the DHS Security Program for DHS facilities, information, and personnel. The CSO is a senior agency official and reports to the Under Secretary for Management on all matters pertaining to security of facilities, information, and personnel. The CSO is a senior agency official who reports directly to the Deputy Secretary on all matters pertaining to facility and personnel security within the DHS.

The responsibilities of the CSO include:

1. DHS information systems that control physical access are approved by the DHS CSO to operate in accordance with this policy document, whether they connect to other DHS information systems or not.
2. Serves as the AO for all systems automating or supporting physical access controls or appoints an AO for each of those systems.

5.1.15 DHS Chief Privacy Officer

The DHS Chief Privacy Officer is the head of the DHS Privacy Office and is responsible for establishing, overseeing the implementation of, and issuing guidance on DHS privacy policy. The DHS Chief Privacy Officer ensures that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of Personally Identifiable Information (PII). The responsibilities of the DHS Chief Privacy Officer include oversight of all privacy activities within the Department, and ensuring compliance with privacy laws, regulations, and policies.

The DHS Chief Privacy Officer coordinates with the CIO and the CISO to provide guidance regarding information technology and technology-related programs and to develop and implement policies and procedures to safeguard PII used or maintained by the Department in accordance with federal law and policy. The DHS Chief Privacy Officer coordinates with Component Privacy Officers and Privacy PPOC with policy compliance at the Component level.

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Departmental information. The DHS Chief Privacy Officer

has exclusive jurisdiction over the development of policy relating to Personally Identifiable Information (PII) and to privacy-sensitive programs, systems, or initiatives. Questions from Components concerning privacy-related policy should be directed to the Component Privacy Office or Privacy Point of Contact (PPOC). If the Component does not have a Privacy Office or PPOC, then please contact the DHS Privacy Office (privacy@dhs.gov; 202-343-1717) or refer to the DHS Privacy Office Web page at www.dhs.gov/privacy for additional information.

The privacy controls in NIST SP 800-53 Rev 4, Appendix J are primarily for use by an organization's Senior Agency Official for Privacy (SAOP) and Chief Privacy Officer when working with program managers, mission and business owners, information owners and stewards, Chief Information Officers, Chief Information Security Officers, information system developers and integrators, and risk executives to incorporate effective privacy protections and practices (i.e., privacy controls) within organizational programs and information systems and the environments in which they operate. The privacy controls facilitate DHS efforts to comply with privacy requirements affecting those department-wide and Component programs and systems that collect, use, maintain, share, or dispose of PII or other activities that raise privacy risks.

Unlike the security controls in NIST SP 800-53 Rev 4, Appendix F, which are allocated to the low, moderate, and high baselines given in Appendix D, the privacy controls in Appendix J are selected and implemented based on DHS privacy requirements and the need to protect the PII collected and maintained by DHS information systems and programs, in accordance with Federal privacy legislation, policies, directives, regulations, guidelines, and best practices.

The responsibilities of the DHS Chief Privacy Officer include:

1. Reviews all Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN), providing approval as appropriate.
2. Leads and oversees the implementation of and compliance with the NIST SP 800-53 Appendix J, "Privacy Control Catalog." Implementation of Appendix J controls is in coordination with the CIO, CISO, program officials, legal counsel, and others as appropriate. No Authority to Operate (ATO) is issued without the DHS Chief Privacy Officer's approval signifying that a system is in compliance with NIST SP 800-53 Appendix J.
3. Establishes and chairs a Data Integrity Board to review all Computer Matching Agreements (CMA).
4. Ensures that the public has access to information about DHS privacy activities and is able to communicate with DHS Privacy Officials; and ensures that privacy practices are publicly available through DHS' public facing website.
5. Implements a process for receiving and responding to complaints, concerns, or questions from individuals about DHS' privacy practices.
6. Implements a process for receiving and responding to complaints, concerns, or questions from individuals about DHS' privacy practices.
7. The DHS Chief Privacy Officer, as the SAOP:

   Develops, implements, and maintains a Department-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the

collection, use, maintenance, sharing, and disposal of PII by programs and information systems.

8. Monitors federal privacy laws and policy for changes that affect the privacy program.
9. Allocates sufficient resources to implement and operate the Department-wide privacy program.
10. Develops a strategic Department privacy plan for implementing applicable privacy controls, policies, and procedures.
11. Develops, disseminates, and implements operational privacy policies and procedures via the DHS 112 process that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.
12. Updates privacy plans, policies, and procedures biennially.
13. Oversees privacy incident management, to include providing guidance to Components, and where appropriate coordination with Components responding to suspected or confirmed privacy incidents.
14. Coordinates with the DHS CIO, DHS CISO, the DHS ESOC, and senior management regarding privacy incidents.
15. Convenes and chairs incident response teams, such as the Privacy Incident Response Team (PIRT) and the Core Management Group (CMG).
16. Reviews and approves all Department Privacy Compliance Documentation, including PTAs, PIAs, and SORNs.
17. Designates Privacy Sensitive Systems as part of the Risk Management Framework based on approved PTAs. Privacy Sensitive Systems are those that maintain PII.
18. Ensures that the Department meets all reporting requirements mandated by Congress or OMB regarding DHS activities that involve PII or otherwise impact privacy.
19. Provides department-wide annual and refresher privacy training.

5.1.16 DHS Chief Financial Officer

The DHS Chief Financial Officer (CFO) implements and manages the DHS Financial Program, including oversight of DHS financial systems. The DHS CFO designates financial systems and consults with the DHS CIO to oversee security control definitions for financial systems.

The responsibilities of the CFO include:

1. The DHS CFO, or their designee, is the AO for applicable financial systems and mixed financial systems and consults with the DHS CIO to oversee security control definitions for those systems.
2. The Component CFO is the AO for all applicable financial mission applications managed at the Component level.
3. Designates the financial systems.

4. Publishes a comprehensive list of designated financial systems during the fourth quarter of every fiscal year. (This list is referred to as the CFO Designated Systems List.)
5. All Component security authorizations for CFO-designated systems are approved and signed by the Component CFO.

5.1.17 Program Managers

Program Managers ensure compliance with the applicable Federal laws and DHS policy directives governing the security, operation, maintenance, and privacy protection of information systems, information, projects, and programs under their control. Program Managers are responsible for program-level POA&Ms that may impact one or more systems.

The responsibilities of Program Managers include:

1. Ensures that program POA&Ms are prepared and maintained.
2. Prioritizes security weaknesses for mitigation.
3. Provides copies of program POA&Ms to affected System Owners.
4. Programs considering the use of e-authentication consult their Privacy Officer to determine whether a change is significant enough to warrant a new or updated PTA, thus initiating the review of privacy risks and how they will be mitigated.
5. Reviews, approves, and signs all custom-developed code prior to deployment into production environments. The Program Manager may delegate this authority in writing to another DHS employee. The authority is not delegated to contractor personnel.
6. Ensures that POA&Ms address the following:

i. Known vulnerabilities in the information system

ii. The security categorization of the information system

iii. The specific weaknesses or deficiencies in the information system security controls

iv. The importance of the identified security control weakness or deficiencies

v. The Component's proposed risk mitigation approach, while addressing the identified weaknesses or deficiencies in the security controls and the rationale for accepting certain weaknesses or deficiencies in the security controls

7. Determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.
8. Ensures compliance with SCRM Plans and consider supply chain risks, as identified by the System Owner, when prioritizing security weaknesses for mitigation.

5.1.18 Ongoing Authorization Manager and Operational Risk Management Board

Each Components Ongoing Authorization (OA) Manager is responsible for evaluating and tracking security events for systems operating under the DHS OA Program. The OA Manager has a security clearance and access greater than or equal to the highest level of information contained in Component systems.

The responsibilities of OA Managers include:

1. Accounts for Component risk threshold.
2. Ensures that Component Risk Executives are made aware of new risks and security issues.
3. Facilities collaboration of the Component IT Subject Matter Experts (SMEs) that serve on the Operational Risk Management Board (ORMB). Component ORMBs determine the criticality of security triggers and the impacts of triggers on the security posture of Component systems that are in OA. The ORMB determines the level of each trigger's visibility and recommends to the Component CISO and AO as adjudicators the actions required to mitigate the risks introduced. Refer to the DHS Ongoing Authorization Methodology for more information regarding the ORMB.
4. An OA Manager is designated for every Component by the Component CISO and serve as the POC for all ongoing risk management for all Component systems enrolled in the OA Program.
5. Duties may be assigned as collateral duties for personnel with existing security responsibilities.
6. Ensures that timely analysis (as outlined by the DHS OA Methodology) of identified security events or triggers is provided to the Component ORMB in support of an accountable environment between the ORMB and the OA Manager.
7. The Component CISO appoints the Chair of the Component ORMB.
8. Responsible for tracking security events in the monthly Trigger Accountability Log (TRAL), communicating and recording recommendations for Component CISO consumption, and ensuring at least quarterly communication with the AO on system risks.

5.1.19 Common Control Providers

A Common Control Provider (CCP) is an organizational official responsible for planning, development, implementation, assessment, authorization, and maintenance of common controls.

The responsibilities of a CCP include:

1. Documents all common controls and submits to the AO.
2. Ensures that required assessments of common controls are carried out by qualified assessors with the appropriate level of independence.
3. Documents assessment findings in a Security Assessment Report (SAR).
4. Ensures that POA&Ms are developed for all controls having weaknesses or deficiencies.