	Department of Human Services Online Directives Information System	Index: Revised: Next Review:	POL1911 01/05/2022 01/05/2024

SUBJECT: DHS Information Security Policies

Security Assessment and Authorization Policy

POLICY
This policy establishes the Enterprise Security Assessment and Authorization Policy, for managing risks from inadequate security assessment, authorization, and continuous monitoring of company information assets through the establishment of an effective security planning program. The security planning program helps DHS implement security best practices with regards to enterprise security assessment, authorization, and continuous monitoring.

A. Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. Centers for Medicare & Medicaid Services
3. United States Internal Revenue Service
4. United States Department of Health & Human Services
5. Georgia Technology Authority
6. Social Security Administration

B. References

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, January 2015
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-100 “Information Security Handbook: A Guide for Managers” March 2007
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-37 “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy” Revision 2 December 2018
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-115 “Technical Guide to Information Security Testing and Assessment” September 2008
- Georgia Technology Authority Enterprise Information Security Policy
- United States Internal Revenue Service, IRS Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information
- Centers for Medicare & Medicaid Services, Volume II: Minimum Acceptable Risk Standards for Exchanges
- Social Security Administration (“SSA”) Electronic Information Exchange Security

Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration ("TSSR")

C. Applicability

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by DHS. Any information, not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including e-mail, messages and files) is the property of DHS. All users (DHS employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy

D. Definitions

Plan of Action and Milestones (POA&M) - a remedial action plan (the process of accepting or resolving a risk) which helps the agency to identify and assess information system security and privacy weaknesses, set priorities, and monitor progress toward mitigating the weaknesses.

E. Responsibilities

DHS shall adopt the Security Assessment and Authorization principles established in NIST SP 800-53 "Security Assessment and Authorization," Control Family guidelines, as the official policy for this domain. The following subsections outline the Security Assessment and Authorization standards that constitute this policy. Each DHS Business System is then bound to this policy and shall develop or adhere to a program plan which demonstrates compliance with the policy related to the standards documented.

- **CA-1 Security Assessment and Authorization Procedures:**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing security assessment and authorization controls governing agency IT resources and information systems on the basis of business and security requirements.
    2. Periodic reviews of this policy shall be performed and documented at least within every
       three years, or when there is a **significant change**.
    3. Periodic review of security assessment and authorization procedures shall be performed at least **annually**.
- **CA-2 Security Assessments**
    1. DHS assesses security controls throughout the system development life cycle process, and at a minimum **annually**.
    2. The agency has developed and executes a security assessment plan which addresses:
        a) The scope of the assessment,
        b) Assessment procedure to be used to determine security control effectiveness,
        c) Assessment environment, assessment team, and assessment roles and responsibilities.
    3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy are performed at least **annually** in order to monitor and maintain minimum acceptable control implementation, intended

operational status, and production of desired outcomes.

4. The agency's security state of organization information systems is reported to appropriate organizational officials on an **annual** basis (i.e. senior management, Chief Information Security Officer, etc.).
5. A security assessment report is produced that documents the results of the assessment and the results of the security control assessment are provided to appropriate agency officials (i.e. senior management, Chief Information Security Officer, etc.).

- **CA-3 Systems Interconnections**
  1. DHS explicitly authorizes connections from the information to other information systems through use of the agency's approved and executed Interconnection Security Agreements.
  2. Annual review and update to the agency's Interconnection Security Agreements is performed to ensure security requirements are adequately addressed within the agreement.
  3. A deny-all and allow-by-exception policy is employed for allowing systems that receive, process, store, or transmit sensitive data to include, but is not limited to, Federal Tax Information (FTI), Social Security Administration data, Centers for Medicare and Medicaid Services (CMS) data, etc.
- **CA-5 Plan of Action and Milestones**
  1. DHS maintains and updates an internal Plan of Action and Milestones (POA&M) in order to document the agency's planned remedial actions for correcting weaknesses or deficiencies identified during the agency security controls assessments.
  2. POA&M review is performed, at a minimum, on a **quarterly** basis.
- **CA-6 Security Authorization**
  1. An Authorizing Official, to include agency senior-level executive or manager, is assigned as the authorizing official for the agency's information system.
  2. The Authorizing Official is responsible for authorizing the information system for processing before commencing operations and before an authority to connect is granted.
     a) Authority to connect shall be granted only upon successful completion of the DHS Certification and Accreditation Process.
  3. Security authorizations are reviewed and updated, as necessary, every **three years** or when there is a significant change in data sensitivity, federal or legislation requirements, security violations, and prior to the previous security authorization.
- **CA-7 Continuous Monitoring**
  1. DHS employs a service provider managed configuration management process for agency information system and components. Review of agency-defined metrics regarding the configuration management process and continuous monitoring program is performed on an **annual** basis.
  2. Continuous security control assessments are performed, and a report of the

agency's security state is provided to the agency's Authorizing Official on, at least, an **annual** basis.

3. Ongoing security monitoring of agency-defined metrics in accordance with the agency's continuous monitoring strategy is performed continuously to ensure agency strategy is effective, maintained, and adhered to.

F. History

None

Evaluation

The Office of Information Technology (OIT), upon recommendation of the DHS Chief Information Security Officer (CISO), evaluates this policy annually by:

1. Comparing its content and intent to evolving regulatory compliance standards imposed upon the Agency, such as, IRS 1075, NIST 800-53, and CMS MARS-E.
2. Addressing any deficiencies or gaps discovered during periodic audits conducted by Georgia DOAA or other regulatory bodies, such as, IRS, CMS, SSA, FBI, etc.