	Department of Human Services Online Directives Information System	Index: Effective: Review:	POL1905 09/20/2014 11/02/2019

SUBJECT: DHS Information Security Policies

Identification and Authentication Policy

POLICY

This policy establishes the Enterprise Identification and Authentication Policy, for managing risks from user access (organizational, non-organizational) and authentication into company information assets through the establishment of an effective identification and authentication program. The identification and authentication program helps DHS implement security best practices with regards to identification and authentication into company information assets.

Authority

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

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, April 2013
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-73 “Interfaces for Personal Identity Verification” Revision 3 February 2010
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-63 “Electronic Authentication Guideline” December 2008
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-76 “Biometric Data Specification of Personal Identity Verification” Revision 1 January 2007
- Georgia Technology Authority Enterprise Information Security Policy
- Centers for Medicare & Medicaid Services’ Catalog of Minimum Acceptable Risk Controls for Exchanges

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.

Definitions

None

Responsibilities

DHS shall adopt the Identification and Authentication principles established in NIST SP 800-53 "Identification and Authentication," Control Family guidelines, as the official policy for this domain. The following subsections outline the Identification and Authentication standards that constitute DHS 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.

- **IA-1 Identification and Authentication Policy and Procedures:** DHS shall:
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for providing identification and authentication controls to 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 identification and authentication procedures shall be performed at least **annually**.
- **IA-2 Identification and Authentication (Organizational User)**
    1. DHS requires that all organizational users (or processes acting on behalf of users) are uniquely identified and authenticated prior to accessing agency information systems.
    2. Multi-factor authentication is required for:
        a) All remote network access to privileged and non-privileged accounts for information systems that receive, process, store, or transmit FTI.
        b) Remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.
- **IA-3 Device Identification and Authentication**

  DHS requires that all system devices uniquely identify and authenticate organizational users prior to the establishment of a connection.
- **IA-4 Identifier Management**

  DHS manages information system identifiers for users and devices by:
    1. Requiring and receiving authorization from designated organizational officials which authorize the assignment of a user, group, role, or device identifier.
    2. Selecting and assigning an identifier that uniquely identifies an individual, group, role, or device.
        a) Assignment of individual, group, role, or device identifiers shall ensure that no two users or devices have the same identifier.
    3. Preventing the reuse of identifiers.
    4. Disabling and de-provisioning inactive user IDs after **120 days of inactivity**.
        a) All mainframe system RACF IDs are revoked after **31 days of inactivity**.
        b) Deleting all RACF User IDs that have been inactive, and or not used for more than **90 days** from the mainframe system
- **IA-5 Authenticator Management**

  DHS manages information system authenticators by:
    1. Verifying the identity of the individual, group, role, or device receiving an information system authenticator as part of the initial authenticator distribution.

2. Using unique initial authenticator content established for information system authenticators.
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use.
4. Executing administrative procedures for initial authenticator distribution, for initial authenticator distribution, lost/compromised, or damaged authenticators, and for revoking authenticators.
    a) If a user knows or suspects that their password has been compromised, they shall immediately:
        i. Notify their supervisor.
        ii. Report a known or potential security breach to the GTA Helpdesk.
        iii. Request the GTA Helpdesk reset or change their password, or if self-service password mechanisms are used, immediately change their own password.
5. Prohibiting the use of automated tools for password generation.
6. Ensuring that default content of authenticators (i.e., passwords provided for initial entry to a system) shall be changed before implementation of the information system or component (e.g., routers, switches, firewalls, printers, workstations, servers).
7. Protecting authenticator content from unauthorized disclosure and modification.
8. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.
9. Changing authenticators for group/role accounts when membership to those accounts changes
10. Enforcing minimum password complexity of:
    a) A minimum of **8 characters**
    b) At least **one** numeric and at least **one** special character
    c) A mixture of at least **one** uppercase and at least **one** lowercase letter
    d) Storing and transmitting only encrypted representation of passwords
    e) A minimum lifetime restriction of **one day** is implemented. Users are required to change privileged accounts within every **60 days**; non-privileged accounts within every **90 days;** all Mainframe account passwords are required to be changed within every **30 days.**
11. The re-use of the **last 24 passwords** is prohibited
12. Temporary passwords used for system logon are authorized, and are required to be changed immediately to a permanent password
13. System initialization (boot) settings are password-protected

- **IA-6 Authenticator Feedback**

  The agency obscures feedback of authentication information during authentication processes to protect the information from possible exploitation/use by unauthorized individuals.
    1. Passwords shall be masked upon entry (e.g., displaying asterisks or dots when a user types in a password) and not displayed in clear text.
    2. Feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.
- **IA-7 Cryptographic Module Authentication**

1. All DHS information systems implement approved mechanisms for authentication to a cryptographic module which meet applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication.
2. The encryption functions have been examined in detail and will operate as intended to protect sensitive data, such as, but not limited to, FTI and SSA data.
3. All electronic transmissions of FTI is encrypted using FIPS 140-2 validated cryptographic modules.

- **IA-8 Identification and Authentication (Non-Organizational Users)**
  DHS requires that non-organizational users and processes acting on behalf of non-agency users uniquely identify and authenticate agency information systems.

History
None