FSIS DIRECTIVE

1306.5 Revision2	5/24/16

IDENTIFICATION AND AUTHENTICATION

I. PURPOSE

This directive provides requirements for Agency personnel and computer system managers to follow on how to secure information technology (IT) systems. In addition, it provides requirements to develop, disseminate, and periodically review and update formal procedures to facilitate the implementation of Identification and Authentication (IDAuth) policy and controls. This revision updates references and security controls as stated in the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

II. CANCELLATION

FSIS Directive 1306.5, Revision 1, *Identification and Authentication (IDAUTH),* 12/13/12

III. BACKGROUND

A. IDAuth is the verification and authentication of a person's or process' identity and is the primary step in securing the Agency's information systems. It is critical in ensuring that data processed and stored within the Agency's information systems are protected from unauthorized access.

B. FSIS ensures information security controls are in place to protect FSIS information systems and data in compliance with Public Law 107-347, Title III, *E-Government Act of 2002*; Public Law 93-579, *Privacy Act of 1974*, as amended; and USDA regulations.

C. Public Law 113-283 was signed into law by the President as the *Federal Information Security Modernization Act of 2014* (FISMA). The goals of FISMA include the development of a comprehensive framework to protect the Government's information, operations, and assets. FISMA assigns specific responsibilities to Federal agencies, and particularly to the NIST and the Office of Management and Budget (OMB) in order to strengthen information technology (IT) system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information security risks to an acceptable level.

D. NIST SP 800-53, Revision 4, outlines the controls addressed by IDAuth. The selection and employment of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization. To adhere to the NIST SP 800-53, Revision 4, FSIS is responsible for the ensuring the Agency meets the requirements stated in section V. of this directive.

IV. ROLES AND RESPONSIBILITIES

All requirements in this directive are the responsibility of OCIO, unless otherwise stated.

A. **The Chief Information Officer (CIO).** Supports and promotes IDAuth throughout the Agency.

B. **OCIO Information System Security Program Manager** (**ISSPM).** Ensures compliance of the IDAuth controls and collaborates among organizational entities.

C. **OCIO Service Desk.** The single point of contact for managing IT related issues from creation to resolution that uses an Automatic Call Distribution (ACD) system with interactive menus, intelligent routing, and integrated voicemail. Operates 24 hour a day, 7 days a week to field service requests using a centralized incident system of record. Service requests can be fielded via call processing or user-submitted emails and incidents.

D. **System Owners.** System owners may be from program areas outside of OCIO. They are to assist in the development of detailed operating procedures to satisfy appropriate IDAuth security controls as discussed in section V. of this directive.

E. **System Users.** All employees, to include program areas outside of OCIO, contractors, other Federal agencies, state and local governments, and authorized private organizations or individuals who use FSIS IT resources are to:

1. Be knowledgeable of IDAuth and the requirements in section V. of this directive; and

2. Ensure their duties are performed in accordance with section V. of this directive.

V. NIST SP 800-53, REVISION 4 REQUIREMENTS

A. **IDAuth Organizational Users.**

1. Ensure the information system uniquely identifies and authenticates organizational users or processes acting on behalf of users (e.g., login scripts) before establishing a system connection;

2. Employ the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof to authenticate user identities;

3. Ensure a personal identity verification credential is used in the unique identification and authentication of Federal employees;

4. Employ IDAuth mechanisms at the application and system level (e.g., at system login) for identifying and authenticating users when stricter controls are necessary;

5. Employ multifactor authentication for network access to privileged and non-privileged accounts;

6. Employ multifactor authentication for local access to privileged accounts;

7. Employ multifactor authentication for local access to non-privileged accounts. These requirements are only applicable to HIGH systems. The categorization of “HIGH,” “MODERATE,” or “LOW” is defined in Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*;

8. Employ a secure 2-factor authentication mechanism for network access to privileged accounts;

9. Employ a secure 2-factor authentication mechanism for network access to non-privileged accounts. These requirements are only applicable to HIGH systems;

10. Implement multifactor authentication for 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 and the device meets the security requirements of FIPS PUB, 140-2, *Security Requirements for Cryptographic Modules,* and meets or exceeds the baseline security controls for the device;

11. Implement replay-resistant authentication mechanisms for network access to privileged accounts;

12. Implement replay-resistant authentication mechanisms for network access to non-privileged accounts. These requirements are only applicable to HIGH systems; and

13. Ensure the system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

B. **Device IDAuth.** Ensure the information system uniquely identifies and authenticates laptops, desktop computers, mobile devices and personal digital assistants before a connection is allowed to be established to an information system.

C. **Identifier Management.** Ensure user identifiers are managed by:

1. Uniquely identifying each user;

2. Verifying the identity of each user;

3. Receiving authorization to issue a user identifier from an appropriate organization official;

4. Issuing the user identifier to the intended party or device identifier to the intended device;

5. Disabling the user identifier immediately when a user is terminated or transferred;

6. Disabling the user identifier after 30 days of inactivity; and

7. Preventing reuse of user or device identifiers for 24 iterations, or as defined in the System Security Plan (SSP).

D. **Authenticator Management.**

1. Manage information system authenticators by:

   a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

   b. Defining initial authenticator content;

   c. Ensuring authenticators have sufficient strength of mechanism for their intended use;

   d. Establishing administrative procedures for initial authenticator distribution for lost, compromised, or damaged authenticators, and for revoking authenticators;

   e. Changing default content authenticators upon information system installation;

f. Changing and refreshing authenticators periodically; and

g. Protecting authenticator content from unauthorized disclosure and modifications.

2. Ensure users take reasonable measures to:

   a. Safeguard and maintain possession of their individual authenticators;

   b. Not loan or share authenticators with others; and

   c. Report lost or compromised authenticators immediately.

3. Configure information systems employing password-based authentication to:

   a. Enforce minimum password complexity of organization-defined requirements for case sensitivity, number of characters, mix of upper and lowercase letters, numbers, and special characters, including minimum requirements for each device type;

   b. Enforce at least a change of one character when new passwords are created;

   c. Encrypt passwords in storage and in transmission;

   d. Enforce password minimum of at least 1 day unless an exception by the Service Desk is issued, and not to exceed a maximum of 90 days;

   e. Prohibit password reuse for 24 generations; and

   f. Allow the use of a temporary password for system logons with an immediate change to a permanent password.

4. Configure information systems employing public key infrastructure-based authentication to:

   a. Validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate path information;

   b. Establish user control of the corresponding private key;

   c. Map the authenticated identity to the user account; and

   d. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

5. Require the registration process to receive E-Authentication passwords, RSA Tokens, and other hardware-type access devices be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

6. Employ mechanisms for hardware token-based authentication that satisfies the strength requirements for their intended use.

E. **Authenticator Feedback.** Ensure password information is obscured during the authentication process to protect the information from possible exploitation and use by unauthorized individuals (e.g., displaying asterisks when a user types in a password).

F. **Cryptographic Module Authentication.** Employ mechanisms for authentication to a cryptographic module that meets the requirements of applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

G. **Non-Organizational Users.**

1. Ensure the Information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users), which includes contractors, volunteers, state users, and industry partners;

2. Conduct an e-authentication risk assessment for authentication of public users accessing Federal information systems to protect nonpublic or privacy-related information;

3. Ensure information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies that are sponsored by USDA Agency or Department staff;

4. Ensure information system accepts only Federal Identity Credential and Access Management (FICAM)-approved third-party credentials;

5. Employ only FICAM-approved information system components in all applicable systems to accept third-party credentials; and

6. Ensure the information system conforms to FICAM-issued profiles.

VI. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

FSIS Directive 1300.7, *Managing Information Technology (IT) Resources*, sets forth the FSIS policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and telecommunications equipment. In addition, FSIS Directive 4735.3, *Employee Responsibilities and Conduct*, outlines the disciplinary action that FSIS may take when an employee fails to fulfill responsibilities or adhere to standards of conduct.

VII. QUESTIONS

A. For questions regarding IDAuth, contact the Agency Information System Security Program at: FSIS_Information_Security@fsis.usda.gov.

B. USDA Departmental directives are located at: http://www.ocio.usda.gov/policy-directives-records-forms and FSIS Directives and Notices are located at: http://www.fsis.usda.gov/wps/portal/fsis/topics/regulations.

Assistant Administrator
Office of Policy and Program Development