

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	NUMBER: DR 3545-001
SUBJECT: Information Security Awareness (ISA) Program	DATE: October 25, 2023
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: October 25, 2028

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Scope	1
3. Special Instructions/Cancellations	2
4. Background	3
5. Policy	3
6. Roles and Responsibilities	4
7. Penalties and Disciplinary Actions for Noncompliance	6
8. Policy Exceptions	6
9. Inquiries	6
Appendix A – Acronyms and Abbreviations	A-1
Appendix B – Definitions	B-1
Appendix C – Authorities and References	C-1

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) requirements for the USDA Information Security Awareness (ISA) Program.
- b. This DR guides all USDA personnel to complete ISA or non-information technology (IT) security training and required role-based training (RBT) on an annual basis.

2. SCOPE

- a. This DR applies to all Mission Areas, agencies, and staff offices, and all USDA personnel requiring access to Federal information or USDA information and information

systems. The term “USDA personnel” includes USDA employees, appointees, contractors, partners, interns, fellows, affiliates, and volunteers.

- b. Nothing in this policy alters the requirements for protecting national security systems or information. This includes those identified in the *Federal Information Security Modernization Act of 2014* ([FISMA](#)), policies, and directives, as issued by the Committee on National Security Systems ([CNSS](#)), or by the intelligence community.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This DR supersedes DR 3545-001, *Information Security Awareness and Training Policy*, dated October 22, 2013.
- b. This DR is effective when published. It will remain in effect until superseded or expired.
- c. USDA Mission Areas, agencies, and staff offices will align their procedures with this DR within 6 months of the publication date.
- d. This DR meets the following requirements:
 - (1) *Federal Information Security Modernization Act of 2014*, 44 United States Code (U.S.C.) §§ 3551-3559;
 - (2) Office of Management and Budget (OMB) Circular [A-130](#), *Managing Information as a Strategic Resource*;
 - (3) OMB Memorandum [M-16-17](#), OMB Circular A-123, *Management’s Responsibility for Enterprise Risk Management and Internal Control*;
 - (4) National Institute of Standards and Technology (NIST) [Federal Information Processing Standards Publication \(FIPS PUB\) 200](#), *Minimum Security Requirements for Federal Information and Information Systems*;
 - (5) NIST [Special Publication \(SP\) 800-16](#), *Information Technology Security Training Requirements: A Role- and Performance-Based Model*;
 - (6) NIST [SP 800-50](#), *Building an Information Technology Security Awareness and Training Program*;
 - (7) NIST [SP 800-53](#), Revision 5, *Security and Privacy Controls for Information Systems and Organizations*; and
 - (8) USDA [DR 3620-001](#), *USDA AgLearn Services, Courseware, and Content*.

4. BACKGROUND

- a. The ISA program derives from NIST and National Initiative for Cybersecurity Education (NICE) framework standards in alignment with NIST [SP 800-181, Revision 1](#), *Workforce Framework for Cybersecurity (NICE Framework)*. The ISA Program provides essential knowledge and methods to protect information systems and data. USDA personnel must complete ISA training or non-IT security training before they receive USDA system access.
- b. USDA personnel with significant information security responsibilities (SISR) must also complete RBT. This will support their job competency and help them develop skills tailored to their role.
- c. This DR will guide USDA on implementing the ISA Program for security and privacy training. The Departmental Training System of Record (DTSR) delivers and documents training completed by USDA personnel.

5. POLICY

- a. The ISA Program will require all USDA personnel to complete ISA training or non-IT security training, annually. USDA personnel who fail to meet this requirement will lose access to USDA systems. Upon successful completion of training, access will resume.
- b. The ISA Program will:
 - (1) Expose USDA personnel to tools that promote ISA. These may include staff meetings and forums, digital signage, phishing exercises, and warning messages;
 - (2) Document and analyze lessons learned, control activities, procedures, and tasks;
 - (3) Use qualitative and quantitative data to assess the effectiveness of the program; and
 - (4) Guide process improvement.
- c. The ISA Program training courses will:
 - (1) Inform USDA personnel of the Federal laws, regulations, guidelines, and Departmental directives relating to information security and privacy; and
 - (2) Promote a culture of situational and security awareness.
- d. The DTSR will:
 - (1) Serve as the primary host for ISA training and RBT;

- (2) Store all records of completion, Rules of Behavior, etc.;
- (3) Document the ISA training status of all USDA personnel;
- (4) Generate FISMA training metrics; and
- (5) Retain records in accordance with USDA [DR 3080-001](#), *Records Management* and the National Archives and Records Administration, [General Records Schedule \(GRS\)](#).

6. ROLES AND RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) will:

- (1) Direct the development of the ISA Program to ensure that all USDA personnel receive annual RBT;
- (2) Inform the Secretary of Agriculture, senior executives and managers, system owners, and other stakeholders annually on the progress of the ISA Program implementation as required by NIST SP 800-50;
- (3) Ensure that the ISA Program has adequate funding to maintain training for USDA personnel; and
- (4) Coordinate with the Director of AgLearn to ensure that the DTSR is available and maintained.

b. The USDA Chief Information Security Officer (CISO) will:

- (1) Develop and manage the ISA Program as part of the USDA IT Security Program. The USDA CISO may assign a designee to carry out and oversee this function;
- (2) Direct reviews of the ISA program metrics and the ability of USDA personnel to meet the requirements;
- (3) Deploy funds and resources needed to maintain the ISA Program in the DTSR;
- (4) Ensure that ISA and security RBT course content is updated as needed;
- (5) Ensure each Mission Area, agency, and staff office maintains oversight and compliance with training requirements and this DR; and
- (6) Document and provide annual reports to the CIO on the status and maturity of the ISA Program.

- c. The USDA Mission Area Assistant CIOs will:
 - (1) Ensure their Mission Area personnel complete the Departmental ISA training and any RBT as required by FISMA; and
 - (2) Ensure that the completion of ISA training and RBT is tracked in the DTSR.
- d. USDA Mission Area Assistant CISOs will coordinate with the USDA CISO to manage the ISA Program at the Mission Area level.
- e. Mission Area, Agency, and Staff Office Information Systems Security Managers (ISSM) will:
 - (1) Ensure that all USDA personnel receive the ISA training and RBT for those with SISR;
 - (2) Coordinate with the Mission Area Assistant CIO and procurement personnel to ensure that relevant procurement documents include the USDA training requirement language; and
 - (3) Generate metrics in the DTSR to show who has and has not completed the training. Use the metrics to measure the effectiveness of the program.
- f. The Director of AgLearn or their designee will:
 - (1) Ensure that the DTSR is available and maintained;
 - (2) Ensure that the associated personnel training data is accurate and complete;
 - (3) Maintain supporting documentation of the data recorded in the DTSR system;
 - (4) Ensure that USDA personnel who complete security training using an alternate method (e.g., paper-based training) record course completion in the DTSR;
 - (5) Support the ISA Program in accordance with DR 3620-001;
 - (6) Document and analyze lessons learned on their programs, control activities, procedures, and tasks; and
 - (7) Use this qualitative and quantitative data to assess effectiveness and to guide process improvement.
- g. Contracting Office Representatives will ensure that all contract personnel at USDA complete the ISA training and RBT;

h. USDA Managers and Supervisors will:

- (1) Ensure that their personnel complete annual ISA or non-IT security training and any RBT; and
- (2) Ensure that their personnel report any known violation of this DR to their Mission Area, agency, or staff office ISSM.

i. All USDA Personnel will:

- (1) Complete annual ISA training and any RBT as required; and
- (2) Report any known violation of this ISA program directive to their Mission Area, agency, or staff office ISSM or supervisor.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NONCOMPLIANCE

[DR 4070-735-001](#), *Employee Responsibilities and Conduct, Section 16: Computers*, sets forth USDA-developed policies, procedures, and standards on the use of computers and telecommunications equipment. In addition, [DR 4070-735-001, Section 21: Disciplinary or Adverse Action](#), states:

- a. Any violation of the responsibilities or standards in this DR may be cause for disciplinary or adverse action; and
- b. Any disciplinary or adverse action taken will be consistent with the applicable laws and regulations.

8. POLICY EXCEPTIONS

USDA Mission Areas, agencies, and staff offices will conform to this policy.

9. INQUIRIES

Send any questions or concerns about this DR to the Office of the Chief Information Officer (OCIO) Information Security Center (ISC) via email at SMD-PCB-Policy@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
DR	Departmental Regulation
DTSR	Departmental Training System of Record
E.O.	Executive Order
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
GRS	General Records Schedule
ISA	Information Security Awareness
ISC	Information Security Center (OCIO component)
ISSM	Information Systems Security Manager
IT	Information Technology
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RBT	Role-Based Training
SISR	Significant Information Security Responsibilities
SP	Special Publication
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

Information Security. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. This is to protect information confidentiality, integrity, and availability. (Adapted from: [44 U.S.C. § 3542](#), *Definitions*)

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Adapted from: OMB, Circular A-130)

Training. Teaching people the knowledge and skills that will enable them to perform their jobs more effectively. (Adapted from: NIST, SP 800-16)

APPENDIX C
AUTHORITIES AND REFERENCES

[5 U.S.C. § 2105](#), *Employee*

[44 U.S.C. § 3542](#), *Definitions*

Acquisition.gov, [Federal Acquisition Regulation](#), June 28, 2023

CNSS, [Introducing the CNSS Library](#), May 6, 2016

E-government Act of 2002, [44 U.S.C. § 101](#), *Joint Committee on Printing: Membership*

[Executive Order \(E.O.\) 12968](#), *Access to Classified Information*, August 2, 1995

[E.O. 13556](#), *Controlled Unclassified Information*, November 4, 2010

Federal Information Security Modernization Act of 2014 (FISMA), [44 U.S.C. §§ 3551-3559](#)

Federal Information Technology Acquisition Reform Act, [Public Law 113-291](#), December 19, 2014

The Government Employees Training Act, [5 U.S.C. §§ 4101-4121](#)

NARA, [General Records Schedules \(GRS\)](#) website

NIST, Computer Security Resource Center, [Glossary](#)

NIST, [FIPS PUB 200](#), *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, as amended

NIST, Information Technology Laboratory Bulletin, [How to Identify Personnel with Significant Responsibilities for Information Security](#), June 2010

NIST, [NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management](#), Version 1.0, January 16, 2020

NIST, [SP 800-16](#), *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998, as amended

NIST, [SP 800-30](#), Revision 1, *Guide for Conducting Risk Assessments*, September 2012, as amended

NIST, [SP 800-50](#), *Building an Information Technology Security Awareness and Training Program*, October 2003, as amended

NIST, [SP 800-53](#), Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of December 10, 2020, as amended

NIST, [SP 800-181](#), Revision 1, *Workforce Framework for Cybersecurity (NICE Framework)*, November 2020, as amended

Office of Government Ethics, [5 Code of Federal Regulations \(CFR\) § 2635, et seq.](#), *Standards of Ethical Conduct for Employees of the Executive Branch*

Office of Personnel Management, [5 CFR § 930.301](#), *Information Systems Security Awareness Training Program*, as amended

OMB, Circular [A-130](#), *Managing Information as a Strategic Resource*, July 28, 2016, as amended

OMB, [M-16-17](#), *OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016

OMB, [M-17-12](#), *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017

USDA, [DR 3080-001](#), *Records Management*, August 16, 2016, as amended

USDA, [DR 3300-001](#), *Telecommunications & Internet Services and Use*, March 18, 2016, as amended

USDA, [DR 3505-003](#), *Access Control for Information and Information Systems*, July 17, 2019, as amended

USDA, [DR 3505-005](#), *Cybersecurity Incident Management*, November 30, 2018, as amended

USDA, [DR 3515-002](#), *Privacy Policy and Compliance for Personally Identifiable Information (PII)*, October 30, 2020, as amended

USDA, [DR 3530-006](#), *Scanning and Remediation of Configuration and Patch Vulnerabilities*, June 5, 2019, as amended

USDA, [DR 3620-001](#), *USDA AgLearn Services, Courseware, and Content*, September 9, 2019, as amended

USDA, [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, October 4, 2007, as amended