

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

DEPARTMENTAL REGULATION	NUMBER: DR 3185-004
SUBJECT: Enterprise Zero Trust Architecture	DATE: September 9, 2024
OPI: Office of the Chief Information Officer, Cybersecurity and Privacy Operations Center	EXPIRATION DATE: September 9, 2029

<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	9
7. Penalties and Disciplinary Actions for Noncompliance	13
8. Policy Exceptions	14
9. Inquiries	14
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) policy for transition to a zero trust architecture (ZTA). It guides the USDA to develop, implement, maintain, and document a federally compliant ZTA.
- b. This directive serves as the foundation for USDA Mission Areas, agencies, and staff offices as they develop and implement their own ZTA procedures. Their ZTA procedures will comply with Federal and Departmental requirements and with USDA's zero trust (ZT) posture.

2. SCOPE

- a. This DR applies to all:

- (1) USDA Mission Areas, agencies, staff offices, and personnel who work for or on behalf of USDA. The term “USDA personnel” includes USDA employees, appointees, contractors, partners, interns, fellows, affiliates, and volunteers;
 - (2) Federal information per [DR 3080-001](#), *Records Management*. This includes information in any medium or form. This also includes information generated, collected, provided, transmitted, stored, maintained, or accessed by or on behalf of USDA;
 - (3) Information systems or services (including cloud-based services) USDA personnel use or operate. This also includes systems or services other organizations use or operate on behalf of the USDA, or those the USDA funds. These also include interconnections between or among systems or services; and
 - (4) USDA facilities from which these information systems or services operate. The USDA may own or operate these facilities. This also includes contractor-, subcontractor-, or other organization-owned or operated facilities on behalf of USDA.
- 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), [44 United States Code \(U.S.C.\) § 3551, et seq.](#) This also includes those identified in [Committee on National Security Systems \(CNSS\)](#) policies, directives, instructions, and standards, as well as intelligence community policies, directives, and instructions.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This DR is effective immediately when published. This DR will remain in effect until it is superseded or expires.
- b. All USDA Mission Areas, agencies, and staff offices will align their ZTA procedures with this policy within 6 months of the publication date.
- c. This DR addresses and meets the requirements of:
 - (1) [7 Code of Federal Regulations \(CFR\) § 2.32](#), *Chief Information Officer*;
 - (2) [44 U.S.C. § 3506\(b\)\(2\)](#), *Federal Agency Responsibilities*;
 - (3) FISMA, 44 U.S.C. § 3551, *et seq.*;
 - (4) National Institute of Standards and Technology (NIST) [Special Publication \(SP\) 800-207](#), *Zero Trust Architecture*;

- (5) Office of Management and Budget (OMB) Circular [A-130](#), *Managing Information as a Strategic Resource*;
- (6) OMB Memorandum [M-19-26](#), *Update to the Trusted Internet Connections (TIC) Initiative*;
- (7) OMB [M-22-09](#), *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*; and
- (8) OMB [M-23-10](#), *The Registration and Use of .gov Domains in the Federal Government*.

4. BACKGROUND

OMB M-22-09 sets forth a Federal ZTA strategy requiring Federal agencies to meet specific cybersecurity standards and objectives by the end of fiscal year 2024. These tasks reinforce the government's defenses against increasingly sophisticated and persistent cyber threat campaigns. ZTA provides a defensible environment using five pillars. The five pillars are Identity, Device, Network, Applications & Workloads, and Data. Within its core tenets, ZTA assumes a threat within the network already exists. Therefore, no user, system, service, or network may access any data without expanded, ongoing device and user authentication.

5. POLICY

- a. The USDA ZTA policy provides requirements to enforce Mission Areas', agencies', and staff offices' responsibilities for managing all information technology (IT) resources.
- b. All Mission Areas, agencies, and staff offices will comply with all Federal laws, policies, requirements, standards, and guidance. They will also follow USDA directives and guidance on ZT.
- c. Mission Areas, agencies, and staff offices will document and analyze lessons learned on their programs, security and privacy control activities, procedures, and tasks. They will use this qualitative and quantitative data to assess effectiveness and guide process improvement.
- d. The five pillars of the ZTA defensible environment include the following requirements:
 - (1) The ZTA Identity pillar principals require a centralized identity management system that integrates into applications and common platforms. This is in accordance with OMB M-22-09 and [DR 3640-001](#), *Identity, Credential, and Access Management (ICAM)*. As part of the ZTA Identity pillar principals and mandated requirements, all USDA staff, contract support, and system support automated

mechanisms must use USDA enterprise-managed identities. The centralized identity management system includes the following components:

- (a) An ICAM program.
 - (b) The ability to:
 - 1 Maintain master user records for all agency users at the enterprise level;
 - 2 Centrally manage the identities, entitlements, and roles of all USDA persons (including USDA personnel, customers, citizens, and nonperson entities);
 - 3 Provide identity life cycle management and identity governance; and
 - 4 Manage access control policies through automated provisioning, management, and governance of both accounts and access entitlements across the USDA enterprise and sub-agency IT systems.
 - (c) An eAuthentication service platform that:
 - 1 Centralizes authentication, federation, identity verification, credentialing, single sign-on, and authorization services for all internal employee-facing, and external citizen-facing, web applications and services, and mobile applications;
 - 2 Supports external identity providers, including other Federal agencies who partner with or obtain services from USDA, as well as citizen-facing identity providers such as [Login.gov](https://login.gov); and
 - 3 Serves as an identity provider to cloud and software-as-a-service applications that USDA uses, or other Federal agency-owned applications USDA personnel must access.
 - (d) Phishing-resistant approaches, such as personal identity verification (PIV) and derived PIV credentials.
 - (e) Fast Identity Online 2 specifications, for use when a PIV or derived PIV is not available. USDA may use these alternative credentials both in network logon and in the USDA eAuthentication platform for applications.
- (2) The ZTA Device pillar requires ongoing, reliable, and complete asset inventories. The approach to keep this information current and accurate comprises hardware asset management (HWAM) and software asset management (SWAM) programs. These programs have the following components and requirements:

- (a) Effective asset management providing visibility of known vulnerabilities on all USDA-owned devices and systems.
- (b) Enforcement of technical controls authorizing and authenticating only known or provisioned devices within the asset inventory.
- (c) HWAM and SWAM data tagged according to the connected network and associated with the relevant Mission Area corresponding to that network.
- (d) HWAM and SWAM asset data and endpoint detection and response (EDR) monitoring agent data. USDA's security information and event management tool receives the data for aggregation. USDA then transmits that data to the Cybersecurity and Infrastructure Security Agency (CISA), conforming to its Continuous Diagnostics and Mitigation program.
- (e) An EDR agent on all managed devices, following these stipulations:
 - 1 The EDR agent only supports managed devices.
 - 2 The following devices do not qualify as managed devices. They need not meet the EDR agent requirement:
 - a Network switches, routers, firewalls, and other network Layers 2 and 3 devices;
 - b Printers and multifunction office machines;
 - c Network performance and management devices;
 - d Kiosks and point-of-sale payment systems;
 - e Cameras, thermostats, lab devices, appliances (e.g., refrigerators), and other networked devices;
 - f Facility access controllers, door controls, card readers, and keypads; and
 - g Smart displays.
- (3) The ZTA Network pillar must resolve domain name system (DNS) queries using encrypted DNS. The Network pillar enforces authenticated hypertext transfer protocol secure (HTTPS) traffic. All USDA Mission Areas, agencies, and staff offices must make technical accommodations to meet the following requirements:

- (a) USDA uses HTTPS for all traffic. This includes external web traffic, application programming interface traffic, internal traffic, mobile applications, and other endpoints.
- (b) Systems enable protective DNS.
- (c) All networks within USDA enterprise networks, systems, and applications will undergo segmentation according to data sensitivity level or business functions.
- (d) The CISA-protected DNS service will replace vendor-managed DNS service.
- (e) Internal DNS infrastructure will use encrypted DNS.
- (f) Endpoint browsers will use DNS over HTTPS. They will also use DNS over transport layer security (TLS). Group policy defines the allowable DNS endpoint list:
 - 1 Endpoints not connected to the USDA virtual private network (VPN) service will use the CISA-protected DNS endpoints as their DNS servers;
 - 2 Endpoints connected to the USDA VPN service will use the USDA enterprise DNS servers as if they were connected inside USDA; and
 - 3 Security measures will block all non-CISA DNS endpoints or non-USDA enterprise DNS endpoints.
- (g) All data owners responsible for traffic traversing over port 80 (hypertext transfer protocol (HTTP)) must configure their sites with certificates.
- (h) All USDA-owned .gov domains will conform to OMB M-23-10.
- (i) The software-defined wide area network (SD-WAN) and TIC 3.0 adoption must distribute security at the network edge for all inbound and outbound traffic. SD-WAN supports the following:
 - 1 User and device authentication via multi-factor authentication (MFA) before connecting;
 - 2 Identity-based and role-based access policy; and
 - 3 Segmented access via security group tagging and VPN segmentation.
- (j) Any implementation of deprecated cryptographic keys must be decommissioned.

- (k) Standard encryption protocols must be upgraded to the latest version if applicable (i.e., TLS 1.3).
- (l) When mission-critical legacy systems are unable to support the latest encryption protocol, these systems will be macro- or micro-segmented through networking protocols. Personnel must submit a plan to migrate any sensitive data the legacy system stores or processes to an updated and encryption capable system within 6 months. They will submit the plan to their Mission Area Assistant Chief Information Security Officer (CISO).
- (4) The ZTA Applications & Workloads pillar requires hosted application programming code analysis via automated inspection, when technically feasible. When automated inspection is not technically feasible, manual expert analysis is acceptable. Refer to OMB M-22-09 about immutable workloads. The Applications & Workloads pillar has the following additional requirements:
 - (a) Code-based vulnerability analysis and inspection will occur prior to the release of a new functionality into production environments.
 - 1 Detected vulnerability reports will include at a minimum these data points:
 - a Operating system;
 - b Hosting platform;
 - c Library dependencies;
 - d Database access; and
 - e Vulnerability impact (low, medium, high, or critical).
 - 2 Personnel must resolve all vulnerabilities before a new functionality is promoted to production.
 - (b) Conduct configuration scans on hosted applications. Ensure there are no deviations from the approved baseline in any authorized micro-segment.
 - (c) All web-hosted or internet-accessible applications and their tools on each site will:
 - 1 Protect using a web application firewall;
 - 2 Conduct dynamic application security testing via continual vulnerability and configuration scans;

- 3 Scan for easily identifiable and reportable vulnerabilities. This meets public vulnerability disclosure requirements per OMB [M-20-32](#), *Improving Vulnerability Identification, Management, and Remediation*. This also meets Department of Homeland Security (DHS) [Binding Operational Directive \(BOD\) 20-01](#), *Develop and Publish a Vulnerability Disclosure Policy*;
 - 4 Maintain an accurate, comprehensive, and frequently updated inventory for visibility of accessible attack surfaces. Incorporate the vulnerabilities into the configuration management database. Integrate this into all USDA Mission Areas, agencies, and staff offices; and
 - 5 Conduct monthly vulnerability scans of the enterprise network from the internet. Report scan results to the information security coordinator.
 - (d) The chartered Cloud Working Group (CWG) is the primary point of contact and key stakeholder responsible for planning and testing automated dynamic code analysis for hosted applications. The team consists of four sub-teams: technical and tactical, strategy, policy, and acquisition.
 - (e) Across all Mission Areas, agencies, and staff offices, all vulnerability visibility within data centers and cloud service providers will be granular, down to the continuous integration and delivery pipelines.
- (5) The ZTA Data pillar requires data classification, robust data tagging, data at rest and in-transit encryption, data governance, and data loss prevention. The Data pillar has the following additional requirements:
 - (a) Personnel will categorize, by specific agency or theme, documents containing sensitive information and created in Microsoft 365.
 - (b) A document categorization strategy group consists of:
 - 1 Chief Data Officer;
 - 2 Office of the General Counsel; and
 - 3 Office of Homeland Security and Privacy.
 - (c) Mission Areas, agencies, and staff offices will analyze data, implement a labeling schema, and protect sensitive data through direct encryption or by storing the documents in a secure storage location.
 - (d) For systems storing sensitive data in the cloud, use independently managed encryption and decryption services.

- (e) CWG will help identify the capabilities, gaps, and methods to monitor unexpected or anomalous decryption requests.
- (f) Mission Areas, agencies, and staff offices will be responsible for developing, implementing, and enforcing training specific to labeling and categorizing data within their purview.

6. ROLES AND RESPONSIBILITIES

a. The Secretary of Agriculture will:

- (1) Direct the heads of Mission Areas, agencies, and staff offices to implement ZTA plans and procedures, provide qualified personnel, and provide other resources;
- (2) Ensure responsible personnel notify and consult with internal and external parties in the mandated time periods. Notifications include strategic decisions, enterprise ZT capabilities, actual or suspected criminal activity or misuse, insider threats, and incidents affecting national security systems. This must be in accordance with Federal and Departmental requirements as part of the ZT implementation strategy; and
- (3) Ensure the USDA Chief Information Officer (CIO) and USDA CISO submit the reports showcasing the progression of cybersecurity maturity.

b. The CIO will:

- (1) Direct the development of ZTA to ensure all USDA personnel only have access to Federal information appropriate to their roles and duties;
- (2) Ensure USDA personnel can meet Federal ZTA requirements; and
- (3) Provide annual reports on ZTA effectiveness to the Secretary of Agriculture, senior leadership, System Owners, data custodians, and other stakeholders. Provide annual reports on the progress of the ZTA implementation. Ensure communication of the concepts, goals, and strategy.

c. The CISO will:

- (1) Develop, implement, manage, monitor, and oversee the implementation of ZTA as part of the USDA IT Security Program. Ensure it complies with Federal laws, regulations, and guidelines, as well as USDA policies. The CISO may assign a designee to carry out and oversee this function;
- (2) Establish, coordinate, and manage a network of ZTA points of contact across all Mission Areas;

- (3) Ensure each Mission Area maintains oversight and compliance with ZTA requirements and this DR; and
 - (4) Document and provide annual reports to the CIO on the status and maturity of the ZTA.
- d. Mission Area Assistant CIOs will:
- (1) Ensure the provisions of this policy are implemented for the information resources supporting the operations and assets under their control;
 - (2) Ensure personnel in their area of responsibility perform their ZTA responsibilities, including notification and reporting, in a timely manner and in accordance with Federal and Departmental requirements;
 - (3) Oversee the Mission Area ZTA implementation based on the Departmental program and in compliance with FISMA. All ZT requirements must meet or exceed the requirements of this DR;
 - (4) Fund, establish, implement, and maintain the Mission Area, agency, and staff office ZT program to include resources, capabilities, ZT capability testing, and training of incident management personnel;
 - (5) Ensure provision of management support and resources. Ensure assignment of those resources to agency and staff office ZT personnel;
 - (6) Ensure their organization develops, documents, implements, reviews, updates, and approves a ZT plan and associated procedures. Those documents must align with Departmental policies, programs, and procedures and comply with Federal policies, regulations, standards, and guidelines for incident reporting and management;
 - (7) Provide direction and guidance to Mission Area, agency, and staff office personnel for:
 - (a) Compliance with Federal laws and requirements pertaining to ZTA and reporting; and
 - (b) Compliance with Departmental ZT policy and procedure and other USDA policies and procedures impacted by ZT implementation.
 - (8) Ensure USDA's enterprise inventory system has a current and accurate inventory of all IT devices and systems in the scope of its responsibility. Identify high value assets to support ZTA.

- e. Mission Area Assistant CISOs will coordinate with the CISO to implement, manage, and oversee ZTA implementation at the Mission Area level.
- f. Information System Security Managers (ISSM) will:
 - (1) Coordinate with personnel who prepare procurement documents to ensure the documents contain ZTA requirements and implementation;
 - (2) Ensure their personnel take annual, role-based ZT training, when required; and
 - (3) Participate in ZT assessments and after-action reports, when required.
- g. System Administrators responsible for maintaining ZTA will:
 - (1) Configure and update ZTA to secure critical assets and data from malicious activity. This includes but is not limited to:
 - (a) Full adoption of MFA;
 - (b) Continuous access evaluation;
 - (c) Implementation of identity and access management;
 - (d) Mature device identity and access control;
 - (e) Configuration of network micro-segmentation as directed;
 - (f) Upgrades to TIC 3.0, or higher;
 - (g) Enforcement of encrypted DNS;
 - (h) Ensuring hosted applications enforce least privilege and separation of duties;
 - (i) Enabling data classification, robust data tagging, high-value data encryption, and data loss protection; and
 - (j) Thorough testing of any service or security setting that could cause a risk to confidentiality, integrity, or availability.
 - (2) Ensure the system reflects the correct number of assigned personnel;
 - (3) Ensure the accuracy of the system, software, and device list; and
 - (4) Maintain supporting documentation of the data recorded in the system.
- h. System Owners will:

- (1) Follow the procedures for incidents or violations of security and privacy policy per [DR 3505-005](#), *Cybersecurity Incident Management*. Work with ZT architects to identify automated triggers that could dynamically block access if an automated alert occurs; and
- (2) Protect USDA information resources regularly with automated detection tools using updated indicators from three main sources:
 - (a) Tool vendors;
 - (b) Cyber Defense Operations Division branches, specifically the Cybersecurity Watch Branch (CWB) and the Cybersecurity Threat Hunt and Intelligence Branch (CTHIB); and
 - (c) The United States Computer Emergency Readiness Team (US-CERT).
- i. Contracting Officer Representatives will ensure all contract personnel follow ZT requirements.
- j. Contractors, Service Providers, or others acting for or on behalf of USDA will:
 - (1) Comply with all Federal and Departmental incident management policies, regulations, guidelines, and procedures indicated in the document governing the relationship;
 - (2) Protect USDA information resources regularly with automated detection tools. Tools will use updated tool vendor, CTHIB, or US-CERT provided indicators. Review the tool analysis results. Provide the results to CWB or other authorized parties; and
 - (3) Report all suspected and actual incidents in the required time frame via methods indicated in the document governing the relationship.
- k. USDA Managers and Supervisors will:
 - (1) Ensure their personnel follow the ZTA requirements as a condition for gaining and maintaining access to USDA systems per [DR 3505-003](#), *Access Control for Information and Information Systems*;
 - (2) Ensure their personnel report any known violation of this DR to their ISSMs; and
 - (3) Ensure their personnel review [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, and [DR 3300-001](#), *Telecommunications & Internet Services and Use*, with their supervisor. Ensure this includes guidance on limited personal use of USDA information systems.

1. All USDA personnel will:

- (1) Understand and comply with agency security and privacy policies and procedures;
- (2) Comply with the rules of behavior for the systems and applications to which they have access;
- (3) Work with management to meet ZT requirements;
- (4) Protect their agency's information by monitoring their actions. These actions include but are not limited to:
 - (a) Following proper password usage per DR 3505-003;
 - (b) Using updated antivirus software;
 - (c) Reporting any suspected incidents or violations of security and privacy policy per DR 3505-005; and
 - (d) Following rules established to avoid social engineering attacks and to deter the spread of spam, viruses, and worms.
- (5) Review DR 4070-735-001 and DR 3300-001 with their supervisor. Ensure this includes guidance on limited personal use of USDA information systems.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NONCOMPLIANCE

- a. DR 4070-735-001, Section 16, *Computers*, sets forth USDA policy, procedures, and standards on employee responsibilities and conduct regarding the use of computers and telecommunications equipment.
- b. In addition, DR 4070-735-001, Section 21, *Disciplinary or Adverse Action*, states:
 - (1) Any violation of the responsibilities or standards contained in this DR may be cause for disciplinary or adverse action; and
 - (2) Any disciplinary or adverse action taken will be consistent with the applicable laws and regulations.

8. POLICY EXCEPTIONS

All Mission Areas, agencies, and staff offices will conform to this policy. If any Mission Area, agency, or staff office cannot meet a specific policy requirement, you may request a

policy exception. To do so, contact the Office of the Chief Information Officer (OCIO) Cybersecurity and Privacy Operations Center (CPOC) Security Management Division (SMD) Risk Management Branch via email at POAMProgram@usda.gov. Note that an approved policy exception is an acceptance of risk but does not constitute compliance.

9. INQUIRIES

Send any questions or concerns about this DR to the OCIO CPOC Cyber Policy and Strategy Program via smd-pcb-policy@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

BOD	Binding Operational Directive
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CPOC	Cybersecurity and Privacy Operations Center
CTHIB	Cybersecurity Threat Hunt and Intelligence Branch
CWB	Cybersecurity Watch Branch
CWG	Cloud Working Group
DHS	Department of Homeland Security
DNS	Domain Name System
DR	Departmental Regulation
EDR	Endpoint Detection and Response
E.O.	Executive Order
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HWAM	Hardware Asset Management
ICAM	Identity, Credential, and Access Management
IETF	Internet Engineering Task Force
ISSM	Information System Security Manager
IT	Information Technology
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NSM	National Security Memorandum
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OWASP	Open Web Application Security Project
PIV	Personal Identity Verification
P.L.	Public Law
RFC	Request for Comments
SD-WAN	Software-Defined Wide Area Network
SMD	Security Management Division
SP	Special Publication
SWAM	Software Asset Management
TIC	Trusted Internet Connection
TLS	Transport Layer Security

U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture
VPN	Virtual Private Network
ZT	Zero Trust
ZTA	Zero Trust Architecture

APPENDIX B

DEFINITIONS

Access Control. The process of granting or denying specific requests. Requests can be for obtaining and using information and related information processing services. Requests can also be to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). (Source: CNSS [CNSS Instruction \(CNSSI\) 4009](#), *Committee on National Security Systems (CNSS) Glossary*)

Access Control Policy. High-level requirements that specify how access is managed and who may access information under what circumstances. (Source: NIST [SP 800-192](#), *Verification and Test Methods for Access Control Policies/Models*)

Authentication. Verifying the identity of a user, process, or device. This is often a prerequisite to allowing access to resources in a system. (Source: NIST [SP 800-53](#), Revision 5, *Security and Privacy Controls for Information Systems and Organizations*)

Authorization. Access privileges granted to a user, program, or process. Alternatively, the act of granting those privileges. (Source: CNSSI 4009)

Continuous Delivery. The stage after continuous integration where code changes are deployed to a testing or staging environment after the build stage. Continuous delivery to a production environment involves the designation of a release frequency. This can be daily, weekly, fortnightly, or some other period, based on the nature of the software or the market in which the organization operates. On top of automated testing, there is a scheduled release process, though the application can be deployed at any time by clicking a button. The deployment process in continuous delivery is characterized as manual. However, tasks such as the migration of code to a production server, the establishment of networking parameters, and the specification of runtime configuration data may be performed by automated scripts. (Source: NIST [SP 800-204C](#), *Implementation of DevSecOps for a Microservices-based Application with Service Mesh*)

Continuous Integration. Continuous integration involves developers frequently merging code changes into a central repository where automated builds and tests run. Build is the process of converting the source code to executable code for the platform on which it is intended to run. In the continuous integration or delivery pipeline software, the developer's changes are validated by creating a build and running automated tests against the build. This process avoids the integration challenges that can happen when waiting for release day to merge changes into the release branch. (Source: NIST SP 800-204C)

Device. In automated assessment, a type of assessment object that is either an IP addressable (or equivalent) component of a network or a removable component that is of security significance. (Source: NIST [NIST Interagency Report \(NISTIR\) 8011](#), Volume 1, *Automation Support for Security Control Assessments*)

eAuthentication. Provides secure, convenient access to multiple USDA applications, websites, programs, and benefits that individual customers and employees are authorized to use. (Source: USDA [eAuthentication](#))

Least Privilege. The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that it needs to perform its function. (Source: CNSSI 4009)

Multi-factor Authentication (MFA). An authenticator that provides more than one distinct authenticator factor. One example is a cryptographic authentication device with an integrated biometric sensor that is required to activate the device. (Source: NIST [SP 800-63-3](#), *Digital Identity Guidelines*)

Personal Identity Verification (PIV). A physical artifact (e.g., identity card, “smart” card) issued to a government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation). The claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). PIV requirements are defined in NIST [Federal Information Processing Standards Publication \(FIPS PUB\) 201-3](#), *Personal Identity Verification (PIV) of Federal Employees and Contractors*. (Source: CNSSI 4009)

Sensitive Information. Information, whereby the loss, misuse, or unauthorized access to or modification of, could adversely affect the National interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the *Privacy Act of 1974*, [5 U.S.C. § 552a](#), *Records Maintained on Individuals*. Sensitive information does not include information that has been specifically authorized under criteria established by an Executive Order (E.O.) or an Act of Congress to be kept classified in the interest of National defense or foreign policy. (Source: NIST [SP 800-150](#), *Guide to Cyber Threat Information Sharing*)

Virtual Private Network (VPN). Protected information system link that uses tunneling, security controls, and endpoint address translation giving the impression of a dedicated line. (Source: CNSSI 4009)

Vulnerability. A known weakness in a system, system security procedures, internal controls, or implementation by which an actor or event may intentionally exploit or accidentally trigger the weakness to access, modify, or disrupt normal operations of a system, resulting in a security incident or a violation of the system’s security policy. (Source: CNSSI 4009)

Zero Trust (ZT). A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. (Source: NIST SP 800-207)

Zero Trust Architecture (ZTA). An enterprise’s cybersecurity plan that utilizes ZT concepts and encompasses component relationships, workflow planning, and access policies. A ZT enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan. (Source: NIST SP 800-207)

APPENDIX C
AUTHORITIES AND REFERENCES

[7 CFR § 2.32](#), *Chief Information Officer*

[44 U.S.C. § 3506\(b\)\(2\)](#), *Federal Agency Responsibilities*

CISA, [Cybersecurity & Infrastructure Security Agency](#) website

CNSS, [CNSSI 4009](#), *Committee on National Security Systems (CNSS) Glossary*, March 7, 2022

CNSS, [Committee on National Security Systems](#) website, May 6, 2016

DHS, [BOD 20-01](#), *Develop and Publish a Vulnerability Disclosure Policy*, September 2, 2020

DOTGOV Online Trust in Government Act of 2020, [Public Law \(P.L.\) 116-260](#), December 27, 2020

[E.O. 13526](#), *Classified National Security Information*, December 29, 2009

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

[E.O. 13587](#), *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011

[E.O. 14028](#), *Improving the Nation's Cybersecurity*, May 12, 2021

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

General Services Administration, [Login.gov](#) website

Internet Engineering Task Force (IETF), [Request for Comments \(RFC\): 1034](#), *Domain Names – Concepts and Facilities*, November 1987

NIST, [FIPS PUB 201-3](#), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022

NIST, [NISTIR 8011](#), Volume 1, *Automation Support for Security Control Assessments*, June 2017

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

NIST, [SP 800-61](#), Revision 2, *Computer Security Incident Handling Guide*, August 2012

NIST, [SP 800-63-3](#), *Digital Identity Guidelines*, June 2017

NIST, [SP 800-150](#), *Guide to Cyber Threat Information Sharing*, October 2016

NIST, [SP 800-192](#), *Verification and Test Methods for Access Control Policies/Models*, June 2017

NIST, [SP 800-204C](#), *Implementation of DevSecOps for a Microservices-based Application with Service Mesh*, March 2022

NIST, [SP 800-207](#), *Zero Trust Architecture*, August 2020

NIST, [SP 1800-16](#), *Securing Web Transactions: TLS Server Certificate Management*, June 2020

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

OMB, [M-16-04](#), *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 30, 2015

OMB, [M-19-02](#), *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 25, 2018

OMB, [M-19-26](#), *Update to the Trusted Internet Connections (TIC) Initiative*, September 12, 2019

OMB, [M-20-32](#), *Improving Vulnerability Identification, Management, and Remediation*, September 2, 2020

OMB, [M-21-30](#), *Protecting Critical Software Through Enhanced Security Measures*, August 10, 2021

OMB, [M-21-31](#), *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021

OMB, [M-22-01](#), *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, October 8, 2021

OMB, [M-22-09](#), *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022

OMB, [M-23-02](#), *Migrating to Post-Quantum Cryptography*, November 18, 2022

OMB, [M-23-10](#), *The Registration and Use of .gov Domains in the Federal Government*, February 8, 2023

Open Web Application Security Project (OWASP), [OWASP](#) website

Privacy Act of 1974, [5 U.S.C. § 552a](#), *Records Maintained on Individuals*

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

USDA, [DR 3130-010](#), *United States Department of Agriculture Enterprise Information Technology Governance*, April 20, 2021

USDA, [DR 3170-001](#), *End User Workstation Configurations*, October 13, 2022

USDA, [DR 3180-001](#), *Information Technology Standards*, January 5, 2021

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

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

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

USDA, [DR 3520-002](#), *Configuration Management*, July 17, 2019

USDA, [DR 3565-003](#), *Plan of Action and Milestones Policy*, September 25, 2013

USDA, [DR 3640-001](#), *Identity, Credential, and Access Management*, June 8, 2021

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

USDA, [eAuthentication](#) website

The White House, [National Security Memorandum \(NSM\)-10](#), *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, May 4, 2022