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

DEPARTMENTAL REGULATION	NUMBER: DR 3530-007
SUBJECT: Encryption Security and Public Key Infrastructure	DATE: August 5, 2024
OPI: Office of the Chief Information Officer, Cybersecurity & Privacy Operations Center	EXPIRATION DATE: August 5, 2029

1. PURPOSE

This Departmental Regulation (DR) provides guidance for the secure use of approved cryptography and public key infrastructure (PKI). These are mandatory for systems and communications protection. They work through signing, user authentication, and encryption. The use of encryption and PKI protects United States Department of Agriculture (USDA) information, communication, and data while in use, at rest, or during transmission. This policy will comply with Federal and Departmental requirements for encryption and PKI.

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*, in any medium or form generated, collected, provided, transmitted, stored, maintained, or accessed by or on behalf of USDA;

(3) Information systems, devices, or services (including cloud-based services) used or operated by USDA, contractors and subcontractors, or other organizations on behalf of USDA, and interconnections between or among systems or services; and

(4) Facilities from which these systems, devices, services, and interconnections operate. USDA, a contractor, a subcontractor, or another organization may own or operate these facilities.

b. Nothing in this DR alters the requirements for the protecting national security systems or information. This includes those identified in the Federal Information Security Modernization Act of 2014 (FISMA) and the Committee on National Security Systems (CNSS) policies, directives, instructions, and standards, and Intelligence Community policies, directives, and instructions.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This DR supersedes:

(1) Departmental Manual (DM) 3530-003, *USDA Use of Public Key Infrastructure*, July 15, 2004; and

(2) DM 3530-005, *Encryption Security Standards*, February 17, 2005.

b. This DR is effective immediately when published and will remain in effect until it is superseded or it expires.

c. All Mission Areas, agencies, and staff offices will align their procedures with this DR within 6 months of the publication date.

4. BACKGROUND

a. Executive Order (E.O.) 14028, *Improving the Nation's Cybersecurity*, requires the encryption of data at rest and in transit. USDA requires systems, information, communications, and data to use cryptography to ensure confidentiality and integrity of information.

b. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-175B, Revision 1, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, guides Federal agencies on the use of cryptography, encryption, and PKI.

c. Cryptography relies upon two basic components: an algorithm and a key. The algorithm and key are used together to protect data (e.g., to encrypt the data or generate a digital signature). They are also used together to remove or check the protection (e.g., to decrypt the encrypted data or verify the digital signature).

d. The security of the cryptographic protection relies on the secrecy of the PKI (e.g., the public key and private key). The users' private key is safeguarded. Their public key links to a digitally signed public key certificate. This certificate proves their ownership of both public and private keys. In systems and applications, the certificate and keys represent the user or individual identified by the certificate. A user must have one current key pair for encryption and decryption and a second key pair for digital signature and signature verification.

5. POLICY

Mission Areas, agencies, and staff offices will encrypt all data at rest and in transit through cryptography and PKI:

a. USDA conforms to NIST encryption standards and criteria for USDA networks, endpoints, and user credentials.

b. Mission Areas, agencies, and staff offices will discontinue the use of encryption standards unapproved by NIST within 6 months of the publication of this document.

c. This policy will apply to hardware modules, firmware modules, software modules, hybrid-software modules, and hybrid-firmware modules.

d. Mission Areas, agencies, and staff offices will adopt and transition to algorithms approved in Federal Information Processing Standards Publication (FIPS PUB) 140-3, *Security Requirements For Cryptographic Modules*. This requirement is in accordance with NIST SP 800-131A, Revision 2, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*.

e. When procuring a private certificate authority (CA) platform, Mission Areas, agencies, and staff offices will:

(1) Determine its applicability to business strategies within USDA;

(2) Outline and justify the total cost of developing a PKI, including any associated information technology development costs;

(3) Determine the appropriate level of security; and

(4) Identify risks, benefits, legal and regulatory compliance constraints, and alternatives.

f. Mission Areas, agencies, and staff offices will ensure interoperability of USDA-approved cryptographic, encryption, and PKI standards when procuring new hardware, software, or contracted services.

g. To protect devices and information used to conduct USDA business and mission functions, Mission Areas, agencies, and staff offices will:

(1) Implement full-disk encryption on all portable devices using compliant algorithms;

(2) Encrypt connection traffic for offsite users. This includes portable devices such as smart phones, tablets, and storage devices.

h. Mission Areas, agencies, and staff offices will only use PKI certificates issued with a Department-approved CA:

(1) PKI certificates requiring external or public trust (e.g., transport layer security (TLS) certificate for public-facing websites) must use an approved commercial CA with trust configured by major platform providers (e.g., Microsoft, Google, Apple, Adobe); and

(2) PKI certificates not requiring external trust must be issued from the USDA.

i. Mission Areas, agencies, and staff offices will use Federal Information Processing Standards (FIPS)-validated, National Security Agency-approved cryptography.

j. Commercial products that USDA uses, and USDA-developed applications that enable the use of PKI, will support the following cryptographic algorithms and associated key size, at a minimum:

(1) Secure Hash Algorithm (SHA)-2 family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256) or SHA-3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512);

(2) Rivest-Shamir-Adleman (RSA) 2048 or greater;

(3) Advanced Encryption Standard (AES) 128, 192, and 256;

(4) Elliptic Curve 224, 256, and 384; and

(5) Elliptic Curve Digital Signature Algorithm (ECDSA) 224 and 256.

k. Only use SHA-1 and RSA 1024 if required to validate digital signatures executed in the past and to decrypt objects encrypted in the past using the older algorithms and key sizes.

l. Mission Areas, agencies, and staff offices will exercise control over cryptographic keys. They will ensure:

(1) Protection of all keys against modification, substitution, and destruction;

(2) Protection of secret or private keys against unauthorized disclosure;

(3) Replacement or retirement of cryptographic keys when they reach their expirations or have weak or compromised integrity;

(4) Physical protection of equipment used to synchronize, store, and archive keys; and

(5) Documentation of key escrow procedures, including an electronic key management and recovery system.

m. For high-impact systems, Mission Areas, agencies, and staff offices will take measures, including escrowing of cryptographic keys, to make information available in case of a lost or corrupted key.

n. Mission Areas, agencies, and staff offices will apply encryption key management services to ensure:

(1) Fully automated key management;

(2) Private key confidentiality; and

(3) Encryption of both stored keys and keys in transit.

o. Mission Areas, agencies, and staff offices will select an appropriate cryptographic key size from Federal standards. They will base the selection on:

(1) The strength of security required;

(2) The amount of data processed with the key; and

(3) The cryptographic period of the key.

p. During remote login sessions, Mission Areas, agencies, and staff offices will use approved encryption protocols to transmit data.

q. Mission Areas, agencies, and staff offices will update their local encryption procedures to align with this directive. They will address the following requirements:

(1) Encrypt all USDA data to protect its confidentiality and integrity; and

(2) Control and protect cryptographic keys used for encrypted transmission.

r. Mission Areas, agencies, and staff offices will write encryption key management plans with instructions to:

(1) Generate the key for different cryptographic systems and applications;

(2) Obtain and issue public key certificates;

(3) Distribute keys to approved users, including a description of how users should activate keys when received;

(4) Store keys and access stored keys;

(5) Change or update keys, including issuing guidance on when, how, and why to do so;

(6) Manage compromised keys;

(7) Revoke keys, including deactivating compromised keys or keys of an approved user who leaves or changes responsibilities;

(8) Archive changed or unnecessary keys, noting the use of archived keys only for decryption or data verification;

(9) Recover lost or corrupted keys;

(10) Back up keys;

(11) Destroy keys; and

(12) Track and review key management activities.

s. Mission Areas, agencies, and staff offices will use assurance levels defined by General Services Administration (GSA), Federal Public Key Infrastructure Policy Authority (FPKIPA), Federal Bridge Certification Authority (FBCA) X.509, Version 3.3, *Certificate Policy for the Federal Bridge Certification Authority*, based on the processed data sensitivity for the corresponding certificates:

(1) Rudimentary Assurance Digital Certificate (will not support non-repudiation);

(2) Basic Assurance Digital Certificate (will not support non-repudiation);

(3) Medium Assurance Digital Certificate;

(4) Personal Identity Verification Interoperable Card Authentication; and

(5) Medium Hardware.

t. Only individuals who have an ongoing business need will have access to PKI technology.

u. Mission Areas, agencies, and staff offices will require all personnel with access to the CA to obtain the required level of security clearance.

v. Mission Areas, agencies, and staff offices will remediate weak cryptographic protocols and ciphers identified by the Department of Homeland Security.

w. Mission Areas, agencies, and staff offices will document and analyze lessons learned on their programs, control activities, procedures, and tasks. They will use this qualitative and quantitative data to assess effectiveness and guide process improvement.

6. ROLES AND RESPONSIBILITIES

a. The Chief Information Officer (CIO) will:

(1) Serve as the final approving authority Departmentwide for IT requirements, to include cryptographic, encryption, and PKI Federal standards adoption;

(2) Serve as the Senior Agency Official for Privacy (SAOP) per DR 3515-002, *Privacy Policy and Compliance for Personally Identifiable Information (PII)*; and

(3) Serve as the final approving authority for Mission Areas, agencies, or staff offices requesting policy waivers.

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

(1) Ensure development of a USDA PKI strategy and implementation plan;

(2) Provide technical policies and standards for encryption employed by the USDA;

(3) Ensure periodic reviews of the technical policies and standards;

(4) Ensure development of a USDA encryption strategy and encryption plan for all systems and networks;

(5) Ensure compliance with cryptographic, encryption, and PKI Federal standards;

(6) Make risk-based decisions (RBD) when reviewing requests for policy exceptions by Mission Areas, agencies, and staff offices. Make waiver request recommendations to the USDA CIO; and

(7) Ensure the periodic review of Mission Areas, agencies, and staff offices for compliance with encryption requirements.

c. The Director of the Office of Contracting and Procurement will ensure that contract language meets the requirements of this DR.

d. Mission Area Assistant CIOs will:

(1) Oversee the management of Mission Area principal certification and registration authorities;

(2) Develop a key management plan for all PKI instances under their purview;

(3) Consult with the SAOP as appropriate when assessing exceptions to policy requests;

(4) Ensure that personnel maintain awareness of the provisions in this DR.

(5) Ensure that all system security plans and procedures include encryption among the technical controls; and

(6) Create and update procedures for the secure use of approved encryption protocols.

e. Mission Area Assistant CISOs will:

(1) Ensure authentication and encryption on all connections; and

(2) Conduct periodic oversight reviews to determine compliance with encryption requirements detailed in this DR. Receive reports on any noncompliant encryption algorithms and methods.

f. The Director of the Cybersecurity & Privacy Operations Center (CPOC), Identity Credential & Access Management Division (ICMD), will:

(1) Manage the list of all approved CAs for the USDA environment;

(2) Ensure that the PKI solution goes through a formal security assessment and authorization (A&A) process before its deployment. The PKI solution will also undergo annual risk assessments; and

(3) Approve PKI authorizations.

g. Information Systems Security Managers (ISSM) will remediate noncompliance or submit a waiver request to the Mission Area Assistant CISO for approval. The request will demonstrate the use of the RBD process.

h. The System Administrators and Network Administrators will:

(1) Ensure that encryption complies with this DR and approved Federal standards;

(2) Ensure that encryption of systems that process, store, or transmit operational information, data, and communication on the use of cryptography meet Federal standards; and

(3) Participate in the central management of all Department virtual private network (VPN) connections. Ensure validation of VPN users.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NONCOMPLIANCE

a. DR 4070-735-001, *Employee Responsibilities and Conduct*, Section 16, *Computers*, sets forth USDA policy, procedures, and standards on employee responsibilities and conduct regarding the use of computers and telecommunications equipment. 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.

b. Such disciplinary or adverse action will be consistent with applicable laws and regulations such as Office of Personnel Management regulations, OMB regulations, and the Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.

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, contact the OCIO CPOC Security Management Division, Risk Management Branch via email at POAMProgram@usda.gov to request a policy exception. An approved policy exception is an acceptance of risk but does not constitute compliance.

9. INQUIRIES

Address any inquiries concerning this DR to the OCIO, CPOC via email to SMD-PCB-Policy@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization
AES	Advanced Encryption Standard
CA	Certificate Authority
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CPOC	Cybersecurity and Privacy Operations Center
DM	Departmental Manual
DR	Departmental Regulation
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
E.O.	Executive Order
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FPKIPA	Federal Public Key Infrastructure Policy Authority
GSA	General Services Administration
ICMD	Identity Credential & Access Management Division
ISSM	Information Systems Security Manager
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RBD	Risk-Based Decision
RSA	Rivest-Shamir-Adleman
SAOP	Senior Agency Official for Privacy
SHA	Secure Hash Algorithm
SP	Special Publication
TLS	Transport Layer Security
USDA	United States Department of Agriculture
VPN	Virtual Private Network

APPENDIX B

DEFINITIONS

Advanced Encryption Standard (AES). Developed as a replacement for data encryption standard. The preferred block cipher algorithm for new products. AES is specified in NIST FIPS PUB 197, *Advanced Encryption Standard (AES)*. AES operates on 128-bit blocks of data, using 128-, 192-, or 256-bit keys. (Source: adapted from NIST SP 800-175B, Revision 1)

Algorithm. A clearly specified mathematical process for computation. A set of rules that, if followed, will give a prescribed result. (Source: NIST SP 800-175B, Revision 1)

Cryptographic Key. A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. Examples include:

a. The transformation of plaintext data into ciphertext data;

b. The transformation of ciphertext data into plaintext data;

c. The computation of a digital signature from data;

d. The verification of a digital signature;

e. The computation of a message authentication code (MAC) from data;

f. The verification of a MAC received with data; and

g. The computation of a shared secret that is used to derive keying material.

(Source: NIST SP 800-175B, Revision 1)

Cryptographic Period. The time span during which each key setting remains in effect. (Source: NIST SP 800-175B, Revision 1)

Cryptography. The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. (Source: NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*)

Data. A representation of information as stored or transmitted. (Source: NIST National Institute of Standards and Technology Interagency Report (NISTIR) 4734, *Foundations of a Security Policy for Use of the National Research and Educational Network*)

Decryption. The process of changing ciphertext into plaintext using a cryptographic algorithm and key. (Source: NIST SP 800-175B, Revision 1)

Elliptic Curve Digital Signature Algorithm (ECDSA). A digital signature algorithm (DSA) that is an analog of DSA using elliptic curves. (Source: NIST SP 800-175B, Revision 1)

Encryption. The process of changing plaintext into ciphertext using a cryptographic algorithm for the purpose of security or privacy. (Source: NIST SP 800-175B, Revision 1)

High-Impact System. An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. (Source: FIPS PUB 200)

Identity, Credential, and Access Management (ICAM). Programs, processes, technologies, and personnel used to do several things. First, create trusted digital identity representations of individuals and nonperson entities. Second, bind those identities to credentials that may serve as a proxy for the individual or nonperson entity in access transactions. Third, leverage the credentials to provide authorized access to an agency's resources. (Source: CNSS Committee on National Security Systems Instruction (CNSSI) 4009, *Committee on National Security Systems (CNSS) Glossary*)

Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form. This includes textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. (Source: Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*)

Key Management. The activities involved in the handling of cryptographic keys and other related security parameters (e.g., initialization vectors and counters) during the entire lifecycle of the keys. This includes their generation, storage, establishment, entry and output, and destruction. (Source: NIST SP 800-175B, Revision 1)

Key Size. The length of a key in bits. This term is used interchangeably with "key length." (Source: NIST SP 800-57, Part 1, Revision 5, *Recommendation for Key Management: Part 1 – General*)

Network. A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (Source: NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*)

Public Key Infrastructure (PKI). A framework established to issue, maintain, and revoke public key certificates. (Source: NIST SP 800-175B, Revision 1)

Rivest-Shamir-Adleman (RSA). A public-key algorithm used for key establishment. It is also used for the generation and verification of digital signatures. (Source: NIST SP 800-175B, Revision 1)

APPENDIX C

AUTHORITIES AND REFERENCES

5 Code of Federal Regulations (CFR) Part 2635, *Standards of Ethical Conduct for Employees of the Executive Branch*

Chief Information Officer, 7 CFR § 2.32, as amended

CNSS, CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary*, March 2, 2022

E.O. 13526, *Classified National Security Information*, December 29, 2009

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.*, December 18, 2014, as amended

General Services Administration (GSA), Federal Public Key Infrastructure Policy Authority (FPKIPA), FBCA, X.509, Version 3.3, *Certificate Policy for the Federal Bridge Certification Authority*, November 3, 2023

GSA, FPKIPA, X.509, Version 2.6, *Certificate Policy for the U.S. Federal PKI Common Policy Framework*, November 3, 2023

NIST, FIPS PUB 140-3, *Security Requirements for Cryptographic Modules*, March 22, 2019

NIST, FIPS PUB 186-5, *Digital Signature Standard (DSS)*, February 3, 2023, as amended

NIST, FIPS PUB 197, *Advanced Encryption Standard (AES)*, November 26, 2001, updated May 9, 2023, as amended

NIST, FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 9, 2006, as amended

NIST, NISTIR 4734, *Foundations of a Security Policy for Use of the National Research and Educational Network*, February 1992

NIST, NISTIR 8369, *Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process*, July 2021

NIST, SP 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007, as amended

NIST, SP 800-52, Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, August 2019, 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 800-56B, Revision 2, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*, March 2019, as amended

NIST, SP 800-57, Part 1, Revision 5, *Recommendation for Key Management: Part 1 – General*, May 2020, as amended

NIST, SP 800-57, Part 2, Revision 1, *Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations*, May 2019, as amended

NIST, SP 800-57, Part 3, Revision 1, *Recommendation for Key Management: Part 3 – Application-Specific Key Management Guidance*, January 2015, as amended

NIST, SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003

NIST, SP 800-77, Revision 1, *Guide to IPsec VPNs*, June 2020, as amended

NIST, SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, November 2007, as amended

NIST, SP 800-131A, Revision 2, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, March 2019

NIST, SP 800-133, Revision 2, *Recommendation for Cryptographic Key Generation*, June 2020, as amended

NIST, SP 800-150, *Guide to Cyber Threat Information Sharing*, October 2016

NIST, SP 800-175A, *Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies*, August 2016, as amended

NIST, SP 800-175B, Revision 1, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, March 2020, as amended

Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch,* 5 CFR §§ 2635, *et seq*.

OMB, Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016

OMB, Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017

OMB, Memorandum M-23-02, *Migrating to Post-Quantum Cryptography*, November 18, 2022

USDA, DR 3080-001, *Records Management*, May 16, 2016, as amended

USDA, DR 3445-001, *Media Protection*, October 30, 2019, as amended

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

USDA, DR 3565-003, *Plan of Action and Milestones Policy*, September 25, 2013, as amended

USDA, DR 3575-004, *Information Technology Security Baselines and Security Control Tailoring*, November 21, 2023

USDA, DR 4070-735-001, *Employee Responsibilities and Conduct*, October 4, 2007, as amended

USDA, RBD-SOP-3540-003B, *USDA Standard Operating Procedures on Risk-Based Decision Management*, September 2021, as amended

USDA, *Matrix of NIST SP 800-53B Encryption Requirements*

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