

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

DEPARTMENTAL REGULATION	NUMBER: DR 3300-015
SUBJECT: Secure Communication Systems	DATE: March 22, 2022
OPI: Office of Homeland Security, National Security Systems Program	EXPIRATION DATE: March 22, 2027

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	2
3. Scope	2
4. Policy	2
5. Roles and Responsibilities	4
6. Compliance	8
7. Policy Exceptions	8
8. Inquiries	9
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) defines the United States Department of Agriculture (USDA) requirements for the management and use of secure communication devices, material, and systems that protect Classified National Security Information (CNSI) to ensure that:
 - (1) Secure communication assets are appropriately managed and controlled;
 - (2) The area(s) where equipment is stored or used is approved and accredited by the Office of Homeland Security's (OHS) Personnel and Document Security Division (PDSD) or CNSI Staff (CNSIS);
 - (3) CNSI users are properly trained and made aware of their responsibilities by members of the OHS' National Security Systems Program (NSSP) and OHS/PDSD/CNSIS; and

- (4) The activities of the user community, OHS PDSD, and NSSP are coordinated.
- b. This policy complies with [Executive Order \(EO\) 13526](#), *Classified National Security Information*; Committee on National Security Systems (CNSS) directives, policies, and instructions; National Security Agency (NSA) security doctrines; Intelligence Community Directives (ICD) issued by the Office of the Director of National Intelligence (ODNI); and USDA directives, which establish, implement, and support secure communications for the protection of CNSI. Guidance references are provided in [Appendix C](#), *Authorities and References* of this document.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy supersedes DR 3300-015, *Secure Communications Systems*, dated July 14, 2016, in its entirety.
- b. This policy will remain in effect until superseded or expiration.
- c. All Mission Areas, agencies, and staff offices will align their policies and procedures with this DR within 6 months of its publication date.
- d. CNSI is also referred to as classified information. Confidential business information and proprietary information are not the same as classified information.

3. SCOPE

- a. This policy applies to all USDA secure communications systems (e.g., telephones, mobile telephones, video teleconference systems, servers, laptop and desktop computers, applications, and wireless devices) that are developed, maintained, or operated by USDA Mission Areas, agencies, staff offices, employees, political appointees, contractors, or other individuals working for or on behalf of the USDA.
- b. This policy only applies to classified systems and national security systems used for the transmission and processing of CNSI. [Departmental Manual \(DM\) 3440-001](#), *USDA Classified National Security Information Program Manual*, provides guidance for the protection of CNSI.

4. POLICY

- a. The OHS NSSP will be the primary office in the USDA to acquire and manage all telecommunication, computer, and network systems used to process, transmit, and store CNSI. Mission Areas, agencies, and staff offices that need access to secure communication systems will request support through the USDA NSSP Manager (NSSPM).

- b. Electronic transmission of classified information will be made via secure telephone, secure radio system, secure video teleconferencing system, secure data network, or a secure facsimile device, protected by an NSA-approved controlled cryptographic item (CCI), encryption device, or other NSA-approved architecture.
- c. Only devices validated by NSA and approved by the USDA for the transmission of CNSI will be used in USDA. A list of approved secure communication devices can be obtained by contacting the NSSP Office.
- d. Only authorized personnel may use, install, remove, or relocate any secure, non-mobile communication device without prior approval from the USDA Communications Security (COMSEC) Manager.
- e. Only authorized personnel may use mobile devices for the processing or transmission of CNSI. Users will adhere to the applicable NSA Security Doctrine for mobile devices.
- f. COMSEC devices (e.g., terminals or cryptographic material) may only be issued to specific approved individuals. These devices cannot be re-issued to another individual without first being returned to the USDA COMSEC Manager for proper inventory management.
- g. Secure Equipment and Systems Requests to Process CNSI
 - (1) Mission Areas, agencies, and staff offices requesting CNSI systems will adhere to USDA and Federal policies and regulations for secure equipment. Security guidelines and requirements outlined in DM 3440-001 and [DM 3300-015](#), *Secure Communication Systems* will be met to ensure the security of CNSI.
 - (2) The requesting Mission Area, agency, or staff office will incur the costs associated with the acquisition of the requested system and the Operations and Maintenance (O&M) funding requirements for it.
 - (3) Mission Areas, agencies, and staff offices will identify their requirements for a CNSI system on form [Agriculture Department \(AD\)-3084](#), *Justification for a Classified National Security Information System*, and submit it to the USDA OHS NSSP office, per DM 3300-015. System requests will be reviewed and signed by a Mission Area, agency, or staff office approving authority before the documentation is submitted to the USDA OHS NSSP office.

5. ROLES AND RESPONSIBILITIES

a. The Director of OHS will:

- (1) Ensure secure communication technical assistance is available to Mission Areas, agencies, and staff offices;
- (2) Serve as the Designated Approving Authority (DAA) for information and telecommunication systems used to process CNSI. The DAA will:
 - (a) Review and approve, or disapprove, all CNSI system requests; and
 - (b) Ensure that all applicable assessment and authorization (A&A) processes required for the implementation of the identified technical solution are properly addressed;
- (3) Oversee the USDA OHS NSSP office;
- (4) Designate an NSSPM with oversight responsibility for the development, implementation, and evaluation of the USDA classified information systems A&A program, per the [Committee on National Security Systems Policy \(CNSSP\) 22, Cybersecurity Risk Management Policy](#), dated August 31, 2016;
- (5) Provide sufficient resources to support the USDA NSSP;
- (6) Provide guidance, direction, and oversight for the security of processes and secure communication systems;
- (7) Provide direction, oversight, and concurrence review functions for the USDA A&A process for secure communication systems;
- (8) Review agency and staff office policy exception requests and render decisions per Section 7, *Policy Exceptions*, of this DR;
- (9) Approve or disapprove all requirements and requests for systems used to process CNSI after review of the information provided by PDSD and USDA NSSP; and
- (10) Maintain an oversight role to ensure consistent and effective implementation of secure communication systems.

b. Mission Area, agency and staff office system owners will:

- (1) Coordinate all CNSI telecommunications requirements with the USDA NSSPM;
- (2) Identify and provide initial acquisition funding and O&M funding, as appropriate, to support the requirements;

- (3) Identify a Federal or contractor point of contact (POC), who is knowledgeable in all aspects of the request and can assist the reviewing entities with questions during the request process and review of the documents. The POC will adhere to USDA and Federal policies and regulations regarding the use of the system requested;
- (4) Coordinate with the USDA NSSPM all support agreements for managed CNSI services from non-USDA entities;
- (5) Register CNSI systems with the USDA NSSP office in accordance with DM 3300-015, and provide required resources to complete A&A for the respective classified stand-alone computer systems;
- (6) Consult with the USDA NSSPM to initiate the necessary procurement actions to obtain CCI and system components used for the processing or transmission of CNSI;
- (7) Ensure the protection of CCI, and notify the USDA COMSEC manager within 12 hours of the discovery of the loss of COMSEC keys or equipment used to process or transmit CNSI;
- (8) Notify the USDA NSSPM and PDSD a minimum of 30 calendar days prior to the relocation of any secure communication equipment, to provide ample time to coordinate logistical changes or address security concerns with the OHS PDSD Classified National Security Information Staff;
- (9) Upon request, assist the COMSEC manager with semiannual inventory and equipment maintenance tasks; and
- (10) Contact the USDA COMSEC manager prior to transfer, reassignment, or any absence of the hand receipt holder exceeding 30 calendar days, to allow for a secure transfer of equipment and delegation of responsibility prior to the receipt holder's departure. Failure to properly transfer devices prior to departure may result in a reportable COMSEC incident.

c. The OHS PDSD will:

- (1) Verify the security clearance of all personnel who manage, operate, configure, and certify telecommunication and computer systems used to process CNSI;
- (2) Certify that the identified location has been approved for processing of CNSI;
- (3) Coordinate CNSI information technology matters with the USDA NSSPM;
- (4) Respond to employee questions on protecting classified information or working in a space approved for the processing and discussion of CNSI;

- (5) Perform information risk assessments;
 - (6) Review and approve new CNSI system requests for:
 - (a) The intended purpose or use of a system;
 - (b) Where and how storage will be maintained;
 - (c) Risk assessment findings; and
 - (d) Security operating guidelines;
 - (7) Approve and maintain a copy of the facility equipment inventory; and
 - (8) Approve system and facility standard operating procedures (SOP).
- d. Authorized users will:
- (1) Protect COMSEC devices, cryptographic keys, communication systems, and passwords to prevent access and disclosure to unauthorized personnel;
 - (2) Report the physical loss of a cryptographic key, COMSEC device, or other secure communication system or component used to process CNSI within 12 hours of discovery to the USDA COMSEC manager and PDSD;
 - (3) Complete initial training for each system and COMSEC device when issued;
 - (4) Complete annual device and system refresher security training, as required, based on the type of device or system; and
 - (5) Return or transfer COMSEC equipment to the NSSP office or other authorized person when duties change or upon leaving the organization.
- e. The USDA NSSPM will:
- (1) Hold and maintain a security clearance that allows access to Top Secret/Special Compartmented Information;
 - (2) Oversee all COMSEC accounts within the USDA;
 - (3) Identify, obtain, and remove NSA-issued USDA COMSEC accounts;
 - (4) Serve as the USDA COMSEC Authority, and designate COMSEC user representatives to order encryption device keys for all USDA COMSEC accounts;

- (5) Manage the centralized systems used by Mission Areas, agencies, and staff offices to support CNSI communications;
 - (6) Manage all service and service agreements with non-USDA support departments and Federal agencies from which CNSI information technology service and material are received;
 - (7) Serve as the Information Systems Security Officer for classified standalone computer systems used to process CNSI:
 - (a) Provide guidance and policy;
 - (b) Write and review master system security plans;
 - (c) Review system security plans (SSP) and memoranda of agreement for accuracy and compliance with USDA and Federal directives;
 - (d) Develop user training documentation; and
 - (e) Ensure compliance with the SSP;
 - (8) Serve as the USDA Homeland Secure Data Network (HSDN) Program Manager; and
 - (9) Coordinate with and advise USDA Departmental leadership on all secure communication systems available that meet Continuity of Operations and Continuity of Government requirements.
- f. The USDA COMSEC Manager will:
- (1) Serve as the USDA COMSEC Manager and COMSEC user representative for ordering, receiving, distributing, and inventorying COMSEC key material;
 - (2) Develop the COMSEC SOP to be followed by all USDA NSSP staff and customers;
 - (3) Coordinate the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material assigned to a COMSEC account;
 - (4) Attend the NSA COMSEC Manager Training Course, as required by NSA;
 - (5) Maintain knowledge of the latest national security communication policies, equipment, and future technologies; and
 - (6) Maintain the security clearance level commensurate with the duties and responsibilities of the position.

g. The USDA OHS NSSP staff will:

- (1) Manage the day-to-day operations of the HSDN computer room and conference room facilities in the South Building;
- (2) Serve as the liaison to the Department of State to facilitate communications and manage USDA organizational roles and user profiles for receipt of classified cables;
- (3) Support secure video teleconferences and validate meeting participant clearances with PDSD;
- (4) Ensure that proper security procedures are followed; and
- (5) Direct questions to PDSD regarding proper procedures for the handling, storage, or use of CNSI.

6. COMPLIANCE

[DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16, *Computers*, establishes the USDA's policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and telecommunications equipment. In addition, Section 21, *Disciplinary or Adverse Action*, states:

- a. A violation of any of the responsibilities and conduct standards contained in this DR may be cause for disciplinary or adverse action; and
- b. Disciplinary or adverse action will be affected in accordance with applicable laws and regulations.

7. POLICY EXCEPTIONS

- a. All USDA Mission Areas, agencies, and staff offices will conform to this policy. If, however, a specific policy requirement cannot be met as explicitly stated, a Mission Area, agency, or staff office may submit a waiver request. The waiver request will explain the reason for the request, identify compensating security controls or actions that meet the intent of the policy, and describe how the compensating controls or actions provide a similar or greater level of defense or compliance than the policy requirement.
- b. Mission Areas, agencies, and staff offices will address all policy waiver requests to the Director, USDA Office of Homeland Security and submit the request to OHSEC-NSSP-SupportTeam@usda.gov for review and determination.

8. INQUIRIES

All questions regarding this DR will be directed to the USDA NSSPM or HSDN Support Team at OHSEC-NSSP-SupportTeam@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization
AD	Agriculture Department
CCI	Controlled Cryptographic Item
CFFB	Central Facility Finksburg
CFR	Code of Federal Regulations
CHVP	Cryptographic High Value Product
CMCS	COMSEC Material Control System
CNSI	Classified National Security Information
CNSIS	Classified National Security Information Staff
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
CSS	Central Security Service
DAA	Designated Approving Authority
DM	Departmental Manual
DR	Departmental Regulation
EO	Executive Order
FISMA	Federal Information Security Modernization Act
FOUO	For Official Use Only
HAIBE	High Assurance Internet Protocol Encryptor
HSDN	Homeland Secure Data Network
ICD	Intelligence Community Directive
IS	Information System
KME	Key Management Entity
MSK	Message Signature Key
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSSP	National Security Systems Program
NSSPM	National Security Systems Program Manager
NTISSI	National Security Telecommunications and Information Systems Security Instruction
O&M	Operations and Maintenance
ODNI	Office of the Director of National Intelligence
OHS	Office of Homeland Security
OMB	Office of Management and Budget
PCMCIA	Personal Computer Memory Card International Association
PDS	Protected Distribution System
PDSD	Personnel and Document Security Division
POC	Point of Contact

SCRM	Supply Chain Risk Management
SDNS	Secure Data Network System
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

Authorized User. Any appropriately cleared individual with a requirement to access an information system (IS) for performing or assisting in a lawful government purpose. (Source: Committee on National Security Systems Instruction [\(CNSSI\) 4009](#), *CNSS Glossary*, dated April 6, 2015)

Confidential Business Information. Information which concerns or relates to the trade secrets, processes, operations, style of works, or apparatus, or to the production, sales, shipments, purchases, transfers, identification of customers, inventories, or amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or other organization, or other information of commercial value, the disclosure of which is likely to have the effect of either impairing the International Trade Commission's ability to obtain such information as is necessary to perform its statutory functions, or causing substantial harm to the competitive position of the person, firm, partnership, corporation, or other organization from which the information was obtained, unless the International Trade Commission is required by law to disclose such information. The term "confidential business information" includes "proprietary information." (Source: Adapted from [19 Code of Federal Regulations \(CFR\) § 201.6](#), *Confidential business information*)

Classified Information. See classified national security information. (Source: CNSSI 4009)

Classified National Security Information (CNSI). Information that has been determined, pursuant to EO 13526 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. (Source: CNSSI 4009)

Clearance. Formal security determination by an authorized adjudicative office that an individual is authorized to access, on a need-to-know basis, a specific level of classified information (Top Secret, Secret, or Confidential). (Source: CNSSI 4009)

Command Authority. The command authority is responsible for the appointment of user representatives for a department, agency, or organization and their key and granting of modern (electronic) key-ordering privileges for those user representatives. (Source: CNSSI 4009)

Communications Security (COMSEC). A component of information assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. (Source: CNSSI 4009)

COMSEC Account. Administrative entity, identified by an account number, used to maintain accountability, custody, and control of COMSEC material. (Source: CNSSI 4009)

COMSEC Manager. Individual who manages the COMSEC resources of an organization. (Source: CNSSI 4009)

COMSEC Material. Item(s) designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, modules, devices, documents, hardware, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions. This includes Controlled Cryptographic Item (CCI) equipment, Cryptographic High Value Products (CHVP), and other Suite B equipment, etc. (Source: CNSSI 4009)

Continuity of Government. A coordinated effort within the Federal Government's executive branch to ensure that national essential functions continue to be performed during a catastrophic emergency. (Source: CNSSI 4009)

Controlled Cryptographic Item (CCI). Secure telecommunications or information system, or associated cryptographic component, that is unclassified and handled through the COMSEC Material Control System (CMCS), an equivalent material control system, or a combination of the two that provides accountability and visibility. Such items are marked "Controlled Cryptographic Item" or, where space is limited, "CCI." (Source: CNSSI 4009)

Cryptographic. Pertaining to, or concerned with, cryptography. (Source: CNSSI 4009)

Cryptography. Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. (Source: CNSSI 4009)

Encryption. The cryptographic transformation of data to produce ciphertext. (Source: CNSSI 4009)

Information Assurance. Measures that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Source: CNSSI 4009)

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: CNSSI 4009)

Information Systems Security Officer. Individual assigned responsibility by the senior agency information security officer, authorizing official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (Source: CNSSI 4009)

Key. A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. Usually, this is a sequence of

random or pseudorandom bits used initially to set up and periodically change the operations performed in cryptographic equipment for the purpose of encrypting or decrypting electronic signals, determining electronic counter-countermeasure patterns, or producing another key. (Source: CNSSI 4009)

Risk Assessment. The process of identifying, estimating, and prioritizing risks resulting from the operation of an information system to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. (Source: CNSSI 4009)

Secure Communications. Telecommunications deriving security by the use of NSA-approved products and/or protected distribution systems (PDS). (Source: CNSSI 4009)

System Security Plan (SSP). Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. (Source: CNSSI 4009)

User. Individual, or (system) process acting on behalf of an individual, authorized to access an information system. (Source: CNSSI 4009)

User Representative (COMSEC). The key management entity (KME) authorized by an organization and registered by the Central Facility Finksburg (CFFB) to order asymmetric key (including secure data network system (SDNS) key and message signature key (MSK)). (Source: CNSSI 4009)

APPENDIX C

AUTHORITIES AND REFERENCES

CNSS references and the NSA policy manual may not be accessible on the unclassified network. Please contact the NSSPM to obtain copies of these documents.

[19 CFR § 201.6](#), *Confidential Business Information*

[32 CFR Part 2001](#), *Classified National Security Information*; Implementing regulation for EO 13526

CNSS, Committee on National Security Systems Directive ([CNSSD](#)) [505](#), *Supply Chain Risk Management (SCRM)*, August 1, 2017

CNSS, [CNSSI 1001](#), *National Instruction on Classified Information Spillage*, June 15, 2021

CNSS, [CNSSI 1253](#), *Security Categorization and Control Selection for National Security Systems*, March 27, 2014

CNSS, [CNSSI 3021](#), *Operational Security Doctrine for the AN/CYZ-10/10A Data Transfer Device*, January 10, 2006

CNSS, [CNSSI 3029](#), *Operational Systems Security Doctrine for TACLANE (KG-175)*, April 19, 2006

CNSS, [CNSSI 4000](#), *Maintenance of Communications Security (COMSEC) Equipment*, October 12, 2012

CNSS, [CNSSI 4001](#), *Controlled Cryptographic Items*, (FOUO), May 7, 2013

CNSS, [CNSSI 4003](#), *Reporting and Evaluating Communications Security (COMSEC) Incidents*, (FOUO), June 16, 2016

CNSS, [CNSSI 4004.1](#), *Destruction and Emergency Protection Procedures for COMSEC and Classified Material*, (FOUO), August 2006 with Annex B amended January 10, 2008

CNSS, [CNSSI 4005](#), *Safeguarding COMSEC Facilities and Materials*, (FOUO), August 22, 2011

CNSS, [CNSSI 4009](#), *Committee on National Security Systems (CNSS) Glossary*, April 6, 2015

CNSS, [CNSSI 4031](#), *Cryptographic High Value Products (CHVP)*, September 18, 2019

CNSS, [CNSSP 1](#), *National Policy for Safeguarding and Control of COMSEC Material*, September 30, 2004

CNSS, [CNSSP 3](#), *National Policy for Granting Access to U.S Classified Cryptographic Information*, October 1, 2007

CNSS, [CNSSP 19](#), *National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products*, June 10, 2013

CNSS, [CNSSP 22](#), *Cybersecurity Risk Management Policy*, August 31, 2016

CNSS, [CNSSP 26](#), *National Policy on Reducing the Risk of Removable Media for National Security Systems*, July 22, 2021

[EO 13526](#), *Classified National Security Information*, December 29, 2009

Federal Information Security Modernization Act of 2014 ([FISMA](#)), December 18, 2014, 44 United States Code (U.S.C.) § 3551, *et seq.*

National Institute of Standards and Technology (NIST) [Special Publication \(SP\) 800-53](#), Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 23, 2020, with updates as of December 10, 2020

NSA Central Security Service (NSA/CSS) Policy Manual 3-16, January 23, 2015

Office of the Director of National Intelligence (ODNI), [ICD 503](#), *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, September 15, 2008

ODNI, [ICD 705](#), *Sensitive Compartmented Information Facilities*, May 26, 2010

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

USDA, [AD-3084](#), *Justification for a Classified National Security Information System*, December 2014

USDA, [DM 3300-015](#), *Secure Communication Systems*, November 15, 2021

USDA, [DM 3440-001](#), *USDA Classified National Security Information Program*, June 9, 2016

USDA, [DR 3440-001](#), *USDA Classified National Security Information Program*, June 9, 2016

USDA, [DR 3440-002](#), *Control and Protection of “Sensitive Security Information,”* January 30, 2003

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

USDA, [DR 4600-003](#), *USDA Defensive Counterintelligence and Insider Threat Programs*, July 12, 2021