

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

DEPARTMENTAL MANUAL	NUMBER: DM 3300-015
SUBJECT: Secure Communication Systems	DATE: November 15, 2021
OPI: Office of Homeland Security – National Security Systems Program	EXPIRATION DATE: November 15, 2024

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	2
3. Scope	2
4. Policy	4
5. Procedures	4
a. Acquiring and Maintaining Classified Systems	4
b. Transferring Information to or from a Classified Environment	9
c. Use of Secure Video Teleconferencing	11
d. HSDN User Accounts and Access	11
e. Joint Worldwide Intelligence Communications System Access	14
f. Classified Cyber Security Incidents	15
6. Roles and Responsibilities	17
7. Inquiries	21
Appendix A – Acronyms and Abbreviations	A-1
Appendix B – Definitions	B-1
Appendix C – Authorities and References	C-1

1. PURPOSE

- a. This Departmental Manual (DM) provides United States Department of Agriculture (USDA) guidance at the Departmental, Mission Area, agency, and staff office levels for:
 - (1) Requesting and responsibly managing:
 - (a) Communications and information technology systems used to process or transmit classified national security information (CNSI) throughout its lifecycle; and
 - (b) Equipment, devices, and cryptographic material for secure communications;

- (2) Requesting access to a national security system (NSS) or a network that transmits or processes CNSI;
 - (3) Moving information between classified and unclassified environments; and
 - (4) Responding to classified system incidents, spillage of CNSI, and loss of cryptographic keys or secure communication devices or equipment.
- b. This DM serves as the foundation for USDA Mission Areas, agencies, and staff offices to develop and implement their own procedures for classified systems and CNSI-related activities that comply with Federal and Departmental requirements and are consistent with the overarching guidance provided in this DM.
 - c. This DM is in compliance with [Executive Order \(E.O.\) 13526](#), *Classified National Security Information*; 32 Code of Federal Regulations (CFR) 2001, *Classified National Security Information Implementing Directive for E.O. 13526*; policies and standards issued by the Committee on National Security Systems (CNSS); and Intelligence Community Directives (ICD). Guidance references are provided in [Appendix C](#), *Authorities and References* of this document.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This manual is effective immediately and remains in effect until superseded or expired.
- b. All Mission Areas, agencies, and staff offices must align their procedures with this manual within 6 months of its publication date.

3. SCOPE

- a. This DM applies to all USDA Mission Areas, agencies, staff offices, employees, appointees, contractors, subcontractors, and others who work for or on behalf of USDA, and who access or will access CNSI, or support, or will support, an NSS.
- b. This DM applies to:
 - (1) All personnel who generate, collect, provide, transmit, store, maintain, or access CNSI on or via Communications Security (COMSEC) equipment or systems by or on behalf of USDA;
 - (2) NSS or services developed, maintained, or operated by, for, or on behalf of USDA;
 - (3) NSS or services used for accessing, transmitting, or processing CNSI, whether internal to USDA or externally with other Federal agencies or organizations;

- (4) Secure, classified communications hardware and software:
 - (a) Devices and systems such as telephones, mobile devices, video teleconference systems, servers, laptops, desktops, and wireless devices;
 - (b) Required applications; and
 - (c) Materials or items designed to secure or authenticate communications, such as cryptographic keys, devices, software, or documents.
 - (5) Facilities or spaces within a facility, such as a room or floor, that are approved by Office of Homeland Security (OHS) Personnel and Document Security Division (PDSD) Classified National Security Information Staff (CNSIS) to house these systems, services, or devices and from which these systems and services operate, whether owned or operated by USDA, or owned or operated on behalf of USDA by a contractor, subcontractor, or other organization; and
 - (6) Any space, open area, or facility approved and accredited by OHS/PDSD/CNSIS for CNSI activities where portable, secure communication devices are used.
- c. This DM focuses on NSS and CNSI from the perspective of the OHS National Security Systems Program (NSSP). Other aspects of safeguarding NSS and CNSI are the responsibility of the OHS PDSD, with which OHS NSSP coordinates their activities.
 - d. This DM complements [Departmental Regulation \(DR\) 3440-001](#), *USDA Classified National Security Information Program*, and [DM 3440-001](#), *USDA Classified National Security Information Program Manual*.
 - e. For more detailed procedures on managing cybersecurity incidents affecting classified systems and CNSI, see [DM 3505-005](#), *Cybersecurity Incident Management Procedures*.
 - f. The following terms are used in this document. See [Appendix C](#) for more detail:
 - (1) An NSS may also be referred to as a classified system, a classified information system, or a secure communication system that meets the criteria defined in [CNSS Instruction \(CNSSI\) 4009](#), *Committee on National Security Systems (CNSS) Glossary*. These terms encompass information systems and telecommunications systems and their components. For ease of understanding, the term “classified systems” is used in this document.
 - (2) CNSI may also be referred to as classified information. Confidential business information and proprietary information are not the same as classified information.

- (3) A managed CNSI service is one that is owned or operated by another organization, such as the Department of Homeland Security (DHS), to provide access to or transmission and processing of CNSI.

4. POLICY

The procedures in this DM expand on the policies established by [DR 3300-015](#), *Secure Communication Systems*, which covers:

- a. Appropriate management and control of assets for classified systems and CNSI;
- b. Securing the confidentiality, integrity, and availability of CNSI through coordination with CNSIS;
- c. Coordination of activities at USDA by OHS's NSSP and OHS, Mission Areas, agencies, staff offices, and the user community; and
- d. System and device security awareness training for all personnel who access or use COMSEC equipment or support a classified system.

5. PROCEDURES

- a. Acquiring and Maintaining Classified Systems

This section explains the procedures for requesting, implementing, using, and operating classified systems and devices, or controlled cryptographic items (CCI) encryption devices, including classified stand-alone systems; equipment used to establish classified data network connectivity or secure video teleconferencing; data encryption devices used to protect CNSI; and secure communication devices used to transmit CNSI, such as fixed, mobile, and satellite telephones and radios.

Procedures for using secure video teleconferencing facilities or accessing classified networks are described in the following Procedures Sections 5c through e.

Mission Areas, agencies, and staff offices are responsible for funding the acquisition, implementation, and operations and maintenance (O&M) of these classified devices, as well as the costs for assessment and authorization (A&A).

All classified systems and their components must be operated in facilities or spaces approved and cleared for CNSI activities by OHS PDSD or by a properly delegated USDA Mission Area, agency, or staff office authority, or at a Government facility with which an approved Memorandum of Understanding (MOU) exists by PDSD. The standard operating procedures (SOP) for the cleared facility must include procedures to ensure classified systems are stored and operated in accordance with DM 3440-001.

Portable secure communication devices, such as mobile phones or radios, must be used in accordance with applicable security doctrine and USDA SOPs when deployed in spaces not formally approved for CNSI activities.

The preferred type of classified stand-alone system is a computer with a removable hard drive or laptop that can be stored in a General Services Administration (GSA)-approved security container, which will require that the facility be approved, at a minimum, for closed storage and processing by PDSD. Computers without removable hard drives, or laptops that are not capable of being stored inside a GSA-approved security container, require the facility to be cleared for open storage of CNSI systems at a classification level equal to or higher than the system.

(1) Requesting and Implementing Classified Systems or Devices

- (a) The requesting agency or staff office must complete the Agriculture Department (AD) Form [AD-3084](#), *Justification for a Classified National Security Information System*, in which the system owner identifies the requested system or device and provides a detailed justification and system capabilities for the request.
- (b) OHS NSSP works with the system owner to document the “proposed solution”, which details the requirements for the classified system.
- (c) The system owner obtains the signatures of the agency funding authority and agency approving authority, indicating that the requesting agency or staff office is able to fund the request, along with the amount of funds available. This does not obligate the funds; it only identifies the requestor’s ability to fund the request and ongoing O&M capabilities.
- (d) The requesting agency or staff office submits the signed Form AD-3084 to OHS NSSP, which routes the form to OHS PDSD for review and signature.
- (e) OHS PDSD reviews the proposed solution requests within 20 business days of receipt to determine if the requesting entity can properly safeguard CNSI. OHS PDSD’s review is based on the:
 - 1 Intended purpose of the system and use of classified information;
 - 2 Secure storage requirements and capabilities (where and how storage will be maintained);
 - 3 Security accreditation of the facility and the facility SOP;
 - 4 Security operating guidelines for the equipment;
 - 5 Appropriate security clearances for personnel; and

6 Documented risk assessment.

- (f) OHS PDSD, in its review, identifies the security processes and procedures required before implementation of the proposed system. The requirements may apply to the requestor, the OHS NSSP Manager (NSSPM) or OHS NSSP, or a managed CNSI service provider.
- (g) OHS PDSD validates that security requirements exist prior to the introduction of the proposed system into an accredited space.
- (h) The Director or designee of OHS either approves or disapproves the request to implement the system or solution.
- (i) The Designated Approval Authority (DAA) reviews the form, certifies through signature that the *Information Assurance Risk Management* process, in accordance with [CNSSI 1253](#), *Security Categorization and Control Selection for National Security Systems*, has been completed, and indicates whether the system must undergo A&A.
- (j) Once the solution is approved, OHS NSSP assists the system owner with following proper acquisition procedures; beginning the A&A process, if required; and implementing the solution.
- (k) All CCI-type devices and COMSEC materials must be delivered to the USDA COMSEC Manager, who generates [Standard Form \(SF\) 153](#), *COMSEC Material Report*, and issues the device(s) to the authorized hand receipt holder.
- (l) OHS PDSD updates the facility equipment inventory when the solution is implemented. OHS PDSD also reviews the SOPs for the facility and any SOPs for the system.

(2) A&A of Classified Systems

- (a) Most systems, components, and devices requested are accredited by a Federal partner agency or managed CNSI service provider. The USDA DAA for CNSI systems determines whether to accept the external A&A under reciprocity or to require an internal A&A and documents the decision on AD-3084. The common exception to this is for stand-alone computer systems. For other exceptions, contact the OHS NSSPM.
- (b) The system owner must develop and maintain a detailed system security plan (SSP) for any classified system requiring A&A.

1 The SSP must follow the format and contain the controls outlined in the Master System Security Plan (MSSP) generated by the OHS NSSPM.

- 2 [CNSSI 1253F Attachment 1](#), *Security Overlays Template*, identifies the controls for a NSS, based on its security categorization.
 - 3 [CNSSI 1253F Attachment 5](#), *Classified Information Overlay*, provides additional controls for safeguarding CNSI.
 - 4 The OHS NSSPM and OHS PDSD must review and concur on the SSP.
- (c) The system must successfully undergo a formal A&A before it may be used for operations.
- 1 If there are two classified stand-alone systems, where one is the primary and the other is the alternate or backup, they may be assessed and authorized together as part of a single A&A.
 - 2 Certifiers (the personnel who perform the assessment) must have appropriate security clearances, applicable security training, and approved accounts for the systems to be assessed. When performing the assessment, the certifiers will determine whether the system is properly configured and complies with stated requirements and produce a security assessment report for the DAA.
- (d) Other outputs of the A&A process are the plans of action and milestones (POA&M) to correct any weaknesses identified during the assessment.
- (e) In addition to A&A, the Mission Area, agency, or staff office must complete and submit Form [AD-3081](#), *Classified Stand-alone Computer Registration/Certification* to the USDA COMSEC Manager. The form provides information about the system and personnel and includes attestations about the facility, system, and personnel.
- (f) Relying on the security assessment report and representations on Form AD-3081 by OHS PDSD and the certifiers, the DAA makes a risk-based decision on whether to allow the system to operate. The DAA's signature on Form AD-3081 authorizes processing of CNSI on the system and serves as the authorization to operate (ATO). The authorization will be valid for no longer than 3 years, although the DAA may set a shorter time.

(3) Accessing and Using Classified Systems

- (a) Use of classified devices or equipment is restricted to authorized personnel with appropriate security clearances.
- (b) All users, system administrators, and certifiers must complete initial classified user training and refresher security training.

(c) For classified stand-alone systems:

- 1 Both of the following forms must be completed, submitted, and approved for user, system administrator, and certifier accounts on classified stand-alone computers:
 - a Form [AD-3085](#), *Classified Stand-Alone Computer User Account Authorization*; and
 - b Form [AD-3080](#), *Classified Stand-Alone Computer User Agreement*.
- 2 OHS PDSD approves Form AD-3085.
- 3 The system owner and the Mission Area, agency, or staff office security official approve Form AD-3080.
- 4 All personnel are required to use different passwords for classified and unclassified system accounts. They are also required to use different passwords for accounts on classified systems that have different classification levels (i.e., the password for a system at the Top Secret level must be different from the password for a system at the Secret level).
- 5 Only an individual with a security clearance equal to or higher than the classification of information on the system may serve as system administrator.
- 6 A certifier must have a security clearance equal to or higher than the classification of information on the system and is prohibited from serving as system administrator or user.
- 7 System users are prohibited from performing or having system administration privileges.
- 8 When a user, certifier, or system administrator is no longer eligible for an account on a classified stand-alone system, the system owner must complete Form [AD-3082](#), *Classified Stand-Alone Computer User Account Termination*. As part of the process, a system administrator must attest on the AD-3082 form that the account has been deactivated or removed.

(4) Operating Classified Systems

- (a) If the official recipient (i.e., the hand receipt holder) of a classified device, equipment, or material is being transferred or reassigned, or will be absent for more than 30 calendar days, the system owner must contact the USDA

COMSEC Manager to return the equipment. OHS PDSD must be informed to update the equipment inventory.

- 1 If the device or material is needed by another individual, only the USDA COMSEC Manager is authorized to re-issue and transfer the material. The USDA COMSEC Manager will arrange for a secure transfer of the device or equipment and delegation of responsibility prior to the official recipient's departure. If the equipment is to be transferred to another location, PDSD must pre-approve and accredit the space where the device is to be located.
 - 2 Failure to properly return or transfer the device or equipment prior to departure may result in a reportable COMSEC incident.
- (b) When a device or equipment is no longer needed, the system owner must return it to the USDA COMSEC Manager, with a completed SF153. The USDA COMSEC Manager must properly inventory and account for returned items before they can be re-issued. Mission Areas, agencies, and staff offices are not authorized to re-issue or key the device or equipment to another individual.
 - (c) To remove or relocate classified non-mobile devices or equipment, the system owner must complete and submit form SF153 to the USDA COMSEC Manager. If equipment needs to be relocated, the system owner must provide at least 30 calendar days' advance notice to the USDA COMSEC Manager. This allows time for NSSP coordination with OHS PDSD to address any logistical changes or security concerns. Only authorized personnel with appropriate security clearance can remove or relocate the devices or equipment.
 - (d) As part of ongoing operations, OHS PDSD reviews and approves equipment inventories for the secure facility or space, and conducts compliance and oversight inspections.

b. Transferring Information to or from a Classified Environment

This section discusses procedures for moving data or information between unclassified and classified domains, or from one security domain level to another, such as from unclassified to Secret or from Secret to Top Secret.

A security domain is an environment within system entities that have a single classification or sensitivity level operating under a common security policy, security model, or security architecture. Classification levels include unclassified, controlled, Secret, Top Secret, and Top Secret/Sensitive Compartmented Information (TS/SCI).

(1) Transferring Information from a Classified to an Unclassified Environment

Only sanitized information on a printed document may be transferred from a classified to an unclassified environment, following these steps:

- (a) Create and print a sanitized version of the document by removing all classified information from the document, so the resulting document contains only statements with unclassified (U) markings and insert headers and footers to designate the document as unclassified.
- (b) Two authorized individuals must review the printed document to verify that the document contains no classified information.
- (c) One of those individuals scans the document to the unclassified network, using an unclassified device.

(2) Transferring Information from an Unclassified to a Classified Environment

- (a) Information being transferred from an unclassified environment to a classified network or system must be in the form of a printed document.
- (b) Use a scanner connected to the classified network or system to upload the printed unclassified document.
- (c) Retrieve the document electronically on the classified network or system after the transfer is complete.

(3) Transferring from a Lower-Level Classified Environment to a Higher-Level Classified Environment

- (a) Information being transferred from a lower-level classified environment to a higher-level classified network or system must be in the form of a printed document.
- (b) Use a scanner connected to the higher-level classified network or system to upload the printed document.
- (c) Retrieve the document electronically on the higher-level classified network or system after the transfer is complete.

(4) Managed CNSI Service Provider Information Transfers

Obtain and follow the instructions for the managed CNSI service provider's method and tools for transferring information.

c. Use of Secure Video Teleconferencing

The OHS NSSP staff supports all secure video teleconferencing systems (SVTS) for USDA and maintains the SOPs for SVTS operation and use. USDA has two types of SVTS systems. The Homeland Secure Data Network (HSDN) SVTS is located in Washington, DC, and planned for other locations. The Crisis Management System SVTS is located in various USDA facilities. Contact OHS NSSP for further information.

- (1) Users who need to attend or host a classified secure video teleconference must submit a completed PDSD Reservation Request Form. The form can be requested from PDSD or NSSP.
- (2) Submit the form via email to CNSIS@usda.gov and OHSEC-NSSP-SupportTeam@usda.gov 3 business days prior to the scheduled event.
- (3) PDSD will verify if the space is available, the participants have the appropriate clearance level, and they are allowed unescorted access to the facility. NSSP will coordinate the logistics of the call after PDSD confirms space availability and participant clearance levels.

d. HSDN User Accounts and Access

HSDN is the Secret-level wide area network, owned and managed by DHS, that provides Federal agencies involved in homeland security missions with access to classified information. HSDN services include full-service network operations, collaboration tools, enterprise applications, and common workstation configurations. Personnel who require access to HSDN must apply for an account, which may also be used to access classified State Department cables.

OHS NSSP assists USDA personnel by processing requests for HSDN access and interfacing with DHS on their behalf. All requests for HSDN accounts or HSDN support in general must be sent to the HSDN Support Team in OHS NSSP.

- (1) Obtaining an HSDN Account and HSDN Token
 - (a) The user must work with their information security (IS) Coordinator and PDSD to complete initial and biannual Derivative Classification Training.
 - (b) The new user must complete Form [AD-3083](#), *Justification Request for an HSDN Account*, and obtain the signature of their supervisor.
 - (c) The completed form must be submitted electronically to via e-mail OHSEC-NSSP-SupportTeam@usda.gov.

- (d) OHS NSSP will forward the completed AD-3083 form to the approving authority or the person to whom that authority has been delegated. For HSDN accounts, that authority has been delegated to the OHS PDSD Chief, the Special Security Officer (SSO), and alternate SSO.
 - (e) If the requestor has not received a response within 5 business days, contact OHS NSSP at USDA-HSDN-SupportTeam@usda.gov or 202-720-0594.
 - (f) A user approved for an HSDN account will receive DHS's HSDN Account Request Application Package to complete. The HSDN Support Team is available to assist.
 - 1 Only designated OHS PDSD personnel may complete the Component Security Clearance Verification Block and Derivative Classification Training Block.
 - 2 OHS PDSD can provide a list of personnel authorized to sign the form. Mission Area, agency, and staff office IS Coordinators are not authorized to sign the form. The OHS NSSPM and Deputy NSSPM are authorized to sign the component Mission Area, agency, or staff office's representative block.
 - (g) Upon approval, the HSDN user will be issued a public key infrastructure (PKI) token and must set a personal identification number (PIN) to access HSDN. For questions or issues with the token, or to set or reset the PIN, contact the HSDN Support Team at USDA-HSDN-SupportTeam@usda.gov or 202-720-0594.
 - (h) Another Federal partner department or agency may issue an HSDN PKI token, with prior coordination between the USDA point of contact (POC) for PKI and the other department's PKI POC.
- (2) Maintaining an HSDN Account and PKI Token
- (a) HSDN users are required to login to their accounts every 30 calendar days to maintain an active account.
 - (b) DHS manages HSDN accounts as follows:
 - 1 The account is locked after 45 calendar days of inactivity; and
 - 2 The account is deactivated after 180 calendar days of inactivity.
 - (c) A user whose account is locked or deactivated must contact the HSDN Support Team at OHSEC-NSSP-SupportTeam@usda.gov or 202-720-0594.

- (d) The HSDN PKI token is the property of DHS and is considered a high-value unclassified item. The PIN is classified at the Secret level.
 - 1 The token and PIN are solely for the use of the person to whom the token is issued and must not be shared with anyone else.
 - 2 The token may not be used on an unclassified system; doing so constitutes a reportable violation.
 - 3 Taking the token into a foreign country or into the embassy or consulate of another country is a reportable security violation.
 - 4 Loss, loss of control, suspected or actual compromise of the token, or compromise of the PIN must be reported within 24 hours of detection to OHS NSSP at OHSEC-NSSP-SupportTeam@usda.gov or 202-720-0594.
 - 5 The token must be returned to OHS NSSP upon termination of the account.

(3) Termination or Temporary Suspension of HSDN Accounts

- (a) Notify OHS NSSP within 24 hours when:
 - 1 An HSDN account is no longer needed because the account holder is terminating employment or changing job responsibilities;
 - 2 The security clearance status of the account holder changes; or
 - 3 Use of the account must be restricted for reasons such as conducting an inquiry.
- (b) OHS NSSP processes the account termination or suspension with DHS and restricts access to HSDN facilities.

(4) Facilities Where HSDN Access Is Available

- (a) OHS NSSP operates the HSDN Suite access for the convenience of personnel from Mission Areas, agencies, and staff offices that have HSDN accounts.
 - 1 The USDA South Building, room S100-E, in Washington, DC, is available during normal duty hours, Monday through Friday, 7:30 a.m. until 6:00 p.m. (Eastern Time), excluding Federal holidays, times of approved early release, closure of the Federal Government, or closure of the South Building; and

- 2 HSDN users in Washington, DC, with an urgent need for HSDN access outside normal duty hours may go to the USDA Security Operations Center, South Building, room S310.

(b) Other USDA facilities with HSDN access are:

- 1 The Beacon facility in Kansas City, MO;
- 2 The Animal and Plant Health Inspection Service (APHIS) headquarters facility in the National Capitol Region;
- 3 The Emergency Relocation Facility in Elkins, WV; and
- 4 The APHIS facility in Fort Collins, CO.

(c) DHS maintains HSDN access at Fusion Centers across the United States. OHS NSSP can provide a list of these locations. To obtain access to a Fusion Center, the following steps are required in advance:

- 1 Contact OHS NSSP at OHSEC-NSSP-SupportTeam@usda.gov or 202-720-0594 to coordinate the access request; and
- 2 Contact OHS PDSD at cnsis@usda.gov or 202-720-7373. OHS PDSD will:
 - a Determine if an agreement is required between USDA and DHS for access and, if so, put the agreement in place; and
 - b Pass the user's personnel security clearance verification information to the Fusion Center.

e. Joint Worldwide Intelligence Communications System Access

The Joint Worldwide Intelligence Communications System (JWICS) for processing and transmitting TS/SCI is operated by a managed CNSI service provider.

OHS PDSD personnel serve as the local administrators for this system and handle all aspects of the system and customer support other than cryptographic support. OHS NSSP provides cryptographic support functions for JWICS.

Mission Areas, agencies, and staff offices are required to fund their allocated percentage of the annual O&M costs for JWICS access, working through OHS NSSP, which coordinates with the managed CNSI service provider.

(1) To obtain JWICS access:

- (a) Request initial JWICS access by contacting OHS PDSD at cnsis@usda.gov or 202-720-7373;
 - (b) Complete the JWICS request account package and submit it to OHS PDSD;
and
 - (c) The Director or Deputy Director of OHS will review the submitted package to approve or disapprove the request.
- (2) To modify or terminate JWICS access, contact OHS PDSD at cnsis@usda.gov or 202-720-7373.

f. Classified Cybersecurity Incidents

This section provides a high-level summary of essential information regarding incidents affecting classified systems, spillage of CNSI, and loss of cryptographic keys or COMSEC devices or equipment. More extensive details can be found in DM 3440-001 and, for CNSI spillage, DM 3505-005.

(1) Operational Security Requirements for Reporting

When reporting a classified or potentially classified incident, including spillage of CNSI, utilize operational security discipline for all communication, to minimize further exposure of the incident and damage to CNSI. Specifically:

- (a) Provide only the minimum amount of information to convey that there has been an incident, then request a face-to-face meeting or a secure call;
- (b) Avoid indicating what the information is or its classification, unless using approved secure methods of communication; and
- (c) Only discuss the incident or potential incident with personnel who have a need to know.

(2) Reporting Incidents and Deadlines for Reporting

- (a) The physical loss of a cryptographic key, COMSEC device, or other secure communication system or component used to process CNSI must be reported within 12 hours of discovery to:

- 1 The USDA COMSEC Manager via OHS NSSP; and
- 2 OHS PDSD.

- (b) All actual or suspected cybersecurity incidents affecting a classified system or CNSI must be reported immediately upon discovery, or notification of the incident, to the:
 - 1 Office of the Chief Information Officer – Information Security Center – Cyber Defense Operations Division (OCIO-ISC-CDOD);
 - 2 OHS PDSD;
 - 3 Agency or staff office IS Coordinators, if applicable; and
 - 4 Agency or staff office information security support staff.
 - (c) The OHS SSO also reports incidents to the OCIO-ISC-CDOD.
- (3) Contact Information for Reporting Classified Cybersecurity Incidents
- (a) OCIO-ISC-CDOD: Email cyber.incidents@usda.gov or call 866-905-6890; both are staffed 24x7x365.
 - (b) OHS PDSD: Email cnsis@usda.gov or call 202-720-7373; the phone is staffed Monday through Friday, 7 a.m. until 5 p.m. (Eastern Time).
 - (c) The USDA COMSEC Manager via OHS NSSP: Email OHSEC-NSSP-SupportTeam@usda.gov or call 202-720-0594.
- (4) Responding to Reported Classified Cybersecurity Incident
- (a) OHS PDSD:
 - 1 Determines whether an official investigation is necessary;
 - 2 Contacts the data owner and agrees on steps needed for cleanup; and
 - 3 Notifies and coordinates with the security staff of any affected external network provider.
 - (b) OHS NSSP:
 - 1 Assists and advises in the incident containment and cleanup strategies and activities, if CNSI systems are involved;
 - 2 Coordinates with classified network owners, as appropriate; and
 - 3 Submits a report to OHS PDSD.

(c) The OCIO-ISC-CDOD:

- 1 Coordinates with OHS PDSD on the approved incident containment and cleanup processes; and
- 2 Manages the incident containment and cleanup by:
 - a Investigating the spread of the incident and communicating that information to OHS PDSD; and
 - b Notifying and advising USDA network owners, external network providers, and network administrators how to contain the incident, isolate and protect classified or potentially classified information, and clean up the incident.

6. ROLES AND RESPONSIBILITIES

- a. The Director of the OHS, in the capacity as DAA, will:
 - (1) Review and approve Form AD-3084;
 - (2) Certify that the Information Assurance Risk Management process has been completed and indicate whether the system must undergo A&A;
 - (3) Upon completion of A&A, make a risk-based decision on allowing the system to operate; and
 - (4) Sign Form AD-3081 to authorize processing of CNSI on the system.
- b. The OHS NSSPM serving as the USDA COMSEC Manager will:
 - (1) Review and concur on SSPs for classified systems;
 - (2) Coordinate with managed CNSI service providers; and
 - (3) Sign as the component agency representative on requests for HSDN accounts.
- c. The OHS NSSP Manager will:
 - (1) Assist the system owner or requestor with documenting detailed requirements and the proposed solution for the system;
 - (2) Assist the system owner with implementing the approved solution;

- (3) Coordinate with SVTS facility owners and requestors to schedule secure video teleconferences;
 - (4) Verify PDSD has confirmed all attendees' clearances prior to the start of any secure video teleconference;
 - (5) Operate facilities for HSDN access;
 - (6) Guide users who need access to classified communications systems at Fusion Centers to OHS/PDSD, which will assist in establishing an MOU;
 - (7) Manage HSDN account requests, account terminations and suspensions, and related support processes;
 - (8) Provide cryptographic support functions for JWICS;
 - (9) Provide initial and annual refresher communications system user security training for authorized users; and
 - (10) Assist and advise in containment and cleanup, and coordinate with classified network owners, as appropriate, when an actual or suspected cybersecurity incident is reported.
- d. The OHS Director or Deputy Director will:
- Review and approve or disapprove requests for implementing a classified system or device, based on information from the review by OHS NSSP and OHS PDSD, and JWICS access.
- e. The OHS PDSD Chief will:
- Review and approve or disapprove requests for new CNSI systems and HSDN accounts.
- f. The OHS PDSD Division Chief will:
- (1) Review the proposed solution for a requested system or device, and identify security processes and procedures required to implement the system before approving the introduction of the proposed system into an accredited space;
 - (2) Review and concur on the SSP for the system;
 - (3) Maintain, review, and approve equipment inventories for secure facilities or spaces;
 - (4) Conduct compliance and oversight inspections of facilities and spaces containing classified systems and equipment;

- (5) Manage Fusion Center agreements through DHS, and provide Fusion Centers with security clearance information for properly cleared personnel who require access;
 - (6) Serve as local administrators for JWICS, manage JWICS account accesses and terminations, and provide general JWICS customer support; and
 - (7) Determine whether an official investigation is necessary when an actual or suspected cybersecurity incident is reported, coordinate with the data owner on cleanup strategies, and notify and coordinate with the security staff of any affected external network.
- g. Mission Area, agency, and staff office Funding Authority and Approving Authority will:
- Sign Form AD-3084 indicating the ability to fund the request and the amount of funds available.
- h. The System Owner or Requestor must:
- (1) Complete Form AD-3084 and obtain signoff from the Mission Area, agency, or staff office funding authority and approving authority;
 - (2) Budget for initial and reoccurring A&A of the requested system, unless the system or device is already accredited by another Federal agency;
 - (3) Develop a concept of operations (CONOPS) for the requested system;
 - (4) Collaborate with OHS Nssp to document the detailed requirements and proposed solution for the system;
 - (5) Develop and maintain a detailed SSP for the system;
 - (6) Ensure that the system A&A is completed, with all weaknesses corrected or documented as POA&Ms, prior to system implementation or operation;
- (1) Ensure that all users, system administrators, and certifiers complete all required security training pertinent to the system;
 - (2) Approve accounts for users, system administrators, and certifiers, and ensure that accounts are terminated in a timely manner when someone is or may no longer be eligible for an account; and
 - (3) Submit SF153 to the USDA COMSEC Manager to install, relocate, or remove classified devices or equipment, at least 30 calendar days in advance for relocations.

- i. Certifiers must:
 - (1) Assess whether the system is properly configured and complies with stated requirements; and
 - (2) Produce a security assessment report for the DAA.
- j. Authorized users will:
 - (1) Complete all required security training, both initially and annually, pertinent to the system;
 - (2) Use assigned accounts properly, protect passwords, PINs, and tokens, and return tokens to OHS NSSP upon termination of HSDN accounts;
 - (3) Promptly report to OHS NSSP any loss, loss of control, suspected or actual compromise of an HSDN token, or compromise of an HSDN PIN;
 - (4) Promptly report the loss of a cryptographic key, COMSEC device, or other secure communication system or component to the USDA COMSEC Manager via OHS NSSP, and to OHS PDSD;
 - (5) Promptly report all actual or suspected cybersecurity incidents affecting a classified system or CNSI to (at a minimum) the OCIO-ISC-CDOD, OHS PDSD, and the Mission Area, agency, or staff office IS Coordinator; and
 - (6) Follow proper procedures for transferring information to or from a classified environment.
- k. The OCIO-ISC-CDOD must, when an actual or suspected classified cybersecurity incident is reported:
 - (1) Coordinate with OHS PDSD on the approved incident containment and cleanup processes;
 - (2) Investigate the spread of the incident and communicate that information to OHS PDSD; and
 - (3) Notify and advise USDA network owners, external network providers, and network administrators how to contain the incident, protect CNSI, and clean up the incident.

7. INQUIRIES

Direct all questions regarding this DM to the OHS NSSPM or the HSDN team at OHSEC-NSSP-SupportTeam@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization
AD	Agriculture Department
APHIS	Animal and Plant Health Inspection Service
ATO	Authorization to Operate
CCI	Controlled Cryptographic Item
CDOD	Cyber Defense Operations Division
CFR	Code of Federal Regulations
CHVP	Cryptographic High Value Product
CIO	Chief Information Officer
CMCS	COMSEC Material Control System
CNSI	Classified National Security Information
CNSIS	Classified National Security Information Staff
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
CONOPS	Concept of Operations
DAA	Designated Approval Authority
DHS	Department of Homeland Security
DM	Departmental Manual
DR	Departmental Regulation
E.O.	Executive Order
ECCM	Electronic Counter-Countermeasure
FISMA	Federal Information Security Modernization Act
GSA	General Services Administration
HAIBE	High Assurance Internet Protocol Encryptor
HSDN	Homeland Secure Data Network
IA	Information Assurance
ICD	Intelligence Community Directive
IS	Information Security
ISC	Information Security Center
IT	Information Technology
JWICS	Joint Worldwide Intelligence Communications System
MOU	Memorandum of Understanding
MSSP	Master System Security Plan
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSS	National Security System
NSSP	National Security Systems Program
NSSPM	National Security Systems Program Manager
O&M	Operations and Maintenance

OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OHS	Office of Homeland Security
P.L.	Public Law
PDS	Protected Distribution System
PDSD	Personnel and Document Security Division
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POC	Point of Contact
SCI	Sensitive Compartmented Information
SF	Standard Form
SOP	Standard Operating Procedure
SSO	Special Security Officer
SSP	System Security Plan
SVTS	Secure Video Teleconferencing System
TACLANE	Tactical Local Area Network Encryption
TS/SCI	Top Secret/Sensitive Compartmented Information
U	Unclassified
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

Certifier. Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages. An alternate term is "security control assessor." (Source: CNSSI 4009, adapted)

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

Classified Information Spillage. Security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification or different security category. (Source: CNSSI 4009)

Classified National Security Information (CNSI). Information that has been determined pursuant to Executive Order (E.O.) 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 access, on a need to know basis, to a specific level of classified information (Top Secret, Secret, or Confidential). (Source: CNSSI 4009)

Closed Storage. The storage of classified information in properly secured General Services Administration-approved security containers. (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 Account Manager. An individual designated by proper authority to be responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material assigned to a COMSEC account. This applies to both primary accounts and subaccounts. (Source: CNSSI 4009)

COMSEC Equipment. Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information to its original form for authorized recipients; also, equipment

designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes cryptographic-equipment, crypto-ancillary equipment, cryptographic production equipment, and authentication equipment. (Source: CNSSI 4009)

COMSEC Incident. Any occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information. COMSEC incident includes Cryptographic Incident, Personnel Incident, Physical Incident, and Protective Technology/Package Incident. (Source: CNSSI 4009)

USDA COMSEC Manager. Individual who manages the COMSEC resources of an organization. The more accurate and used term is “COMSEC account manager.” (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)

COMSEC Module. Removable component that performs COMSEC functions in a telecommunications equipment or system. (Source: CNSSI 4009)

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 CFR § 201.6](#), *Confidential business information*)

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, methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. (Source: CNSSI 4009)

Cyber Incident. Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. See also “incident.” (Source: CNSSI 4009)

Designated Approval Authority (DAA). Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with authorizing official, designated accrediting authority, and delegated accrediting authority. (Source: CNSSI 4009)

Domain. An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See security domain. (Source: CNSSI 4009)

Encryption. The cryptographic transformation of data to produce cipher text (data in unintelligible form). (Source: CNSSI 4009, adapted)

Incident. An occurrence that results in actually or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (Source: CNSSI 4009)

Key. A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. Usually, 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, or for determining electronic counter-countermeasures (ECCM) patterns, or for producing other keys. (Source: CNSSI 4009)

Keying Material. Key, code, or authentication information in physical, electronic, or magnetic form. It includes key tapes and list, codes, authenticators, one-time pads, floppy disks, and magnetic tapes containing keys, plugs, keyed microcircuits, electronically generated key, etc. (Source: CNSSI 4009)

National Security System (NSS). Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which:

- a. Involves intelligence activities or cryptologic activities related to national security; or
- b. Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of

Congress to be kept classified in the interest of national defense or foreign policy.
(Source: *Federal Information Security Modernization Act of 2014* ([FISMA](#)), adapted)

NSA-Approved Product. Cryptographic equipment, assembly or component classified or certified by the National Security Agency (NSA) for encrypting and decrypting classified national security information and sensitive information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms. (Source: CNSSI 4009)

Open Storage. Any storage of classified national security information outside of approved containers. This includes classified information that is resident on information systems media and outside of an approved storage container, regardless of whether or not that media is in use (i.e., unattended operations). Open storage of classified cryptographic material and equipment must be done within an approved COMSEC facility, vault, or secure room when authorized personnel are not present. (Source: CNSSI 4009)

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

Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence. (Source: CNSSI 4009)

Spillage. Security incident that results in the transfer of classified information onto an information system not authorized to store or process that information. (Source: CNSSI 4009)

Unclassified. Information that does not require safeguarding or dissemination controls pursuant to [E.O. 13556](#), *Controlled Unclassified Information*, and has not been determined to require protection against unauthorized disclosure pursuant to E.O. 13526, *Classified National Security Information*, or any predecessor or successor Order. (Source: CNSSI 4009, adapted)

APPENDIX C

AUTHORITIES AND REFERENCES

NOTE: CNSS references and the NSA policy manual may not be accessible on the unclassified network. Please contact the OHS NSSPM if you need to obtain a copy of a document.

Classified National Security Information Implementing Directive for E.O. 13526, [32 CFR 2001](#), July 1, 2010

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 1253F Attachment 1](#), *Security Overlays Template*, August 27, 2013

CNSS, [CNSSI 1253F Attachment 5](#), *Classified Information Overlay*, May 9, 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*, (FOUU), May 07, 2013

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

CNSS, [CNSSI 4005](#), *Safeguarding COMSEC Facilities and Materials*, 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, CNSS Policy [\(CNSSP\) 1](#), *National Policy for Safeguarding and Control of COMSEC Material*, September 30, 2004

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

CNSS, [CNSSP 11](#), *National Policy Governing the Acquisition of Information Technology (IT) Products*, July 19, 2021

CNSS, [CNSSP 15](#), *Use of Public Standards for the Secure Information Sharing*, October 20, 2016

CNSS, [CNSSP 19](#), *National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products*, June 1, 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*, June 22, 2021

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

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

[Executive Order 13556](#), *Controlled Unclassified Information*, November 4, 2010

Federal Information Security Modernization Act of 2014, (FISMA), [Public Law \(P.L.\) 113-283](#), December 18, 2014, [codified at 44 United States Code \(U.S.C.\) §§ 3551 et seq.](#)

GSA, [SF153](#), *COMSEC Material Report*, September 1988

National Security Agency Central Security Service (NSA/CSS) Policy Manual 3-16, *Control of Communications Security (COMSEC) Material*, August 5, 2005

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

USDA, [AD-3080](#), *Classified Stand-Alone Computer User Agreement*, December 2014

USDA, [AD-3081](#), *Classified Stand-Alone Computer Registration/Certification*, December 2014

USDA, [AD-3082](#), *Classified Stand-Alone Computer User Account Termination*, December 2014

USDA, [AD-3083](#), *Justification Request for an HSDN Account*, December 2014

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

USDA, [AD-3085](#), *Classified Stand-Alone Computer User Account Authorization*, December 2014

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

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

USDA, [DR 3300-015](#), *Secure Communication Systems*, July 14, 2016, as amended

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

USDA, [DR 3540-003](#), *Security Assessment and Authorization*, August 12, 2014

USDA, OHS, *PDSD Reservation Request Form*