

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

DEPARTMENTAL REGULATION	Number: DR 3300-015
SUBJECT: Secure Communication Systems	DATE: July 14, 2016
	OPI: Office of the Chief Information Officer, Agriculture Security Operations Center

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Scope	2
3. Special Instructions/Cancellations	2
4. Policy	2
5. Secure Equipment and Systems Requests to Process CNSI	3
6. Roles and Responsibilities	4
7. Penalties and Disciplinary Actions for Non-Compliance	8
8. Policy Exceptions	9
9. 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 requirements for the management and use of secure communication devices, material, and systems utilized to protect Classified National Security Information (CNSI). This policy facilitates the management of CNSI systems by providing guidelines to ensure that:
- (1) Secure communication assets are appropriately managed and controlled;
 - (2) The integrity and availability of CNSI is properly secured;
 - (3) CNSI users are properly trained and aware of their responsibilities; and

- (4) The user community, Office of Homeland Security and Emergency Coordination (OHSEC), and National Security System Program (NSSP) activities are coordinated.
- b. This policy complies with Executive Order [\(E.O.\) 13526](#), *Classified National Security Information*; *Committee on National Security Systems* (CNSS) directives, policies, and instructions; National Security Agency (NSA) security doctrines; Intelligence Community Directives (ICDs) issued by the Office of the Director of National Intelligence; and United States Department of Agriculture (USDA) directives, which establish, implement, and support secure communications for the protection of CNSI. Guidance references can be found in Appendix C.

2. SCOPE

- a. This policy applies to all USDA secure communications systems (e.g., telephones, mobile telephones, video teleconference systems, servers, laptops, desktops, applications, wireless devices) developed, maintained, and operated by USDA agencies, staff offices, employees, political appointees, contractors, and 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.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy supersedes DR 3300-001-D, *Secure Telephone*, dated March 23, 1999, in its entirety.
- b. This policy will remain in effect until superseded.
- c. All agencies and staff offices shall align their policies and procedures with this DR within six months of the publication date.
- d. CNSI is also referred to as classified information. Confidential business information and proprietary information are not the same as classified information.

4. POLICY

- a. The Office of the Chief Information Officer (OCIO) Agriculture Security Operations Center (ASOC) NSSP shall be the primary office within USDA to acquire and manage

all telecommunication, computer, and network systems that are utilized to process, transmit, and store CNSI. Agencies and staff offices that need access to secure communication systems shall request support through the USDA NSSP Manager (NSSPM).

- b. All CNSI shall be transmitted 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 USDA for the transmission of CNSI shall be used in USDA. A list of approved secure communication devices can be found in forthcoming *DM Secure Communication Systems*.
- d. Only authorized personnel shall use, install, remove, or relocate any secure, non-mobile communication devices without prior approval from the USDA Communications Security (COMSEC) Manager.
- e. Only authorized personnel shall use mobile devices for the processing and/or transmitting of CNSI. Users must adhere to the applicable NSA Security Doctrine for the mobile devices.
- f. COMSEC devices (e.g., terminals or cryptographic material) shall be issued to specific, approved individuals. The devices shall not be re-issued to another individual without first being returned to the USDA COMSEC Manager for proper inventorying and processing.

5. SECURE EQUIPMENT AND SYSTEMS REQUESTS TO PROCESS CNSI

- a. Agencies and staff offices requesting CNSI systems must adhere to USDA and Federal policies and regulations for secure equipment. Security guidelines and requirements must be met to ensure the security of CNSI in accordance with DM 3440-001 and forthcoming *DM Secure Communication Systems*.
- b. The requesting agency or staff office shall incur the costs associated with the acquisition and Operations and Maintenance (O&M) funding requirements for the requested system.
- c. Agencies and staff offices shall identify their requirements for a CNSI system on form [AD-3084](#), *Justification for a Classified National Security Information System*, and submit it to the USDA NSSP office as outlined in the forthcoming *DM Secure Communication Systems*. System requests shall be reviewed and signed by an agency or staff office approving authority before the documentation is submitted to the USDA NSSP office.

6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) shall:
 - (1) Ensure secure communication technical assistance is available to agencies and staff offices; and
 - (2) Serve as the Designated Approving Authority (DAA) for information and telecommunication systems utilized to process CNSI. This role may be delegated in writing to the Associate Chief Information Officer (ACIO) for ASOC. The DAA shall:
 - (a) Review and approve or disapprove all 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.
- b. The ACIO for ASOC shall:
 - (1) Perform DAA duties as delegated by the USDA CIO;
 - (2) Oversee the USDA NSSP office;
 - (3) Designate an NSSPM with oversight responsibility for the development, implementation, and evaluation of the USDA classified information systems A&A program per Committee on National Security Systems Policy ([CNSSP 22](#), *Policy on Information Assurance Risk Management for National Security System*, dated January 1, 2012, and [CNSSP 22 Amendment 1](#), dated June 17, 2013); and
 - (4) Provide sufficient resources to support the USDA NSSP.
- c. The USDA Chief Information Security Officer (CISO) shall:
 - (1) Provide guidance, direction, and oversight for the security of processes and secure communication systems;
 - (2) Provide direction, oversight, and concurrence review functions for the USDA A&A process for secure communication systems; and
 - (3) Review agency and staff office policy exception requests and render decision per Section 8 of this DR.
- d. Agency and staff office system owners shall:
 - (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 who can assist the reviewing entities with any questions that arise during the request process and review of the documents. The POC must adhere to USDA and Federal policies and regulations regarding the use of the system requested;
 - (4) Coordinate all support agreements for managed CNSI services from non-USDA entities with the USDA NSSPM;
 - (5) Register CNSI systems with the USDA NSSP office in accordance with the forthcoming *DM Secure Communication Systems* and provide required resources to complete an 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 and/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;
 - (8) Notify the USDA NSSPM prior to the relocation of any secure communication equipment. A minimum of 30 calendar days' notice is recommended to provide ample time for coordination with the OHSEC Classified National Security Programs Branch for any logistical changes that may be required and to ensure security concerns are properly addressed;
 - (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 their departure. Failure to properly transfer devices prior to departure may result in a reportable COMSEC incident.
- e. The OHSEC Chief of Personnel and Document Security Division (PDSO) shall:
- (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 about proper procedures for protecting classified information or working in an accredited space for the processing and discussion of CNSI;
 - (5) Perform information risk assessments;
 - (6) Review and approve new CNSI system requests for the following:
 - (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 (SOPs).
- f. The Director or Deputy Director of OHSEC shall:
- (1) 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
 - (2) Maintain an oversight role to ensure consistent and effective implementation of secure communication systems.
- g. Authorized users shall:
- (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 to the USDA COMSEC manager and PDSD within 12 hours of discovery;
 - (3) Complete initial training for each system and/or COMSEC device when issued; and
 - (4) Complete annual refresher security training, as required, based on the type of device or system.
 - (5) Return COMSEC equipment to the NSSP office when duties change or leaving the organization.

h. The USDA NSSPM shall:

- (1) Hold and maintain a Top Secret/Special Compartmented Information security clearance.
- (2) Oversee all COMSEC accounts within the USDA;
- (3) Identify, obtain, and remove NSA-issued USDA COMSEC accounts;
- (4) Serve as the USDA Command Authority, and designate COMSEC user representatives to order encryption device keys for all USDA COMSEC accounts;
- (5) Manage the centralized systems used by agencies and staff offices to support CNSI communications;
- (6) Manage all service and service agreements with non-USDA support departments and Federal agencies from whom 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 (SSPs) 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) Designate a 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/Continuity of Government requirements.

i. The USDA COMSEC Manager shall:

- (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.

j. The USDA NSSP staff shall:

- (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 or the requesting agency's Information Security Coordinator;
- (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.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

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

- (1) A violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action; and
- (2) Disciplinary or adverse action shall be effected in accordance with applicable laws and regulations.

8. POLICY EXCEPTIONS

All USDA agencies and staff offices are required to conform to this policy. However, in the event that a specific policy requirement cannot be met as explicitly stated, agencies and staff offices may submit a waiver request. The waiver request shall explain the reason for the request, identify compensating security controls/actions that meet the intent of the policy, and identify how the compensating controls/actions provide a similar or greater level of defense or compliance than the policy requirement. Agencies and staff offices shall address all policy waiver request memoranda to the USDA CISO and submit the request to USDA-HSDN-SupportTeam@ocio.usda.gov for review and determination.

9. INQUIRIES

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

- END -

APPENDIX A

ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization
ACIO	Associate Chief Information Officer
AD	Agriculture Department
ASOC	Agriculture Security Operations Center
CCI	Controlled Cryptographic Item
CFFB	Central Facility Finksburg
CFR	Code of Federal Regulations
CHVP	Cryptographic High Value Products
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMCS	COMSEC Material Control System
CNSI	Classified National Security Information
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
E.O.	Executive Order
ECCM	Electronic Counter-Measures
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
HAIPE	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
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
O&M	Operations and Maintenance
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OHSEC	Office of Homeland Security and Emergency Coordination

OMB Office of Management and Budget
P.L. Public Law
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
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 [CFR § 201.6](#))

Classified Information. See classified national security information. (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)

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 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 it 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, or for determining electronic counter-measures (ECCM) patterns, or for producing other key. (Source: CNSSI 4009)

Risk Assessment. The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. 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 through the use of NSA-approved products and/or protected distribution systems (PDSs). (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 if you need to obtain a copy of the document.

Confidential Business Information, [19 CFR 201.6](#), April 1, 2011

CNSS, Committee on National Security Systems Directive ([CNSSD](#)) [505](#), *Supply Chain Risk Management (SCRM)*, March 7, 2012

CNSS, [CNSSI 1001](#), *National Instruction on Classified Information Spillage*, February 01, 2008

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*, For Official Use Only (FOUO), October 12, 2012

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

CNSS, [CNSSI 4003](#), *Reporting and Evaluating COMSEC Incidents*, (FOUO), May 27, 2014

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)*, February 16, 2012

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

CNSS, [CNSSP 22](#), *Policy on Information Assurance Risk Management for National Security Systems*, January 2012

CNSS, [CNSSP 22 Amendment](#), *Amendment 1 to Committee on National Security Systems Policy No. 22, dated January 2012*, June 17, 2013

CNSS, [CNSSP 26](#), *National Policy on Reducing the Risk of Removable Media for National Security Systems*, July 24, 2013

CNSS, National Security Telecommunications and Information Systems Security Instruction ([NSTISSI 3028](#)), *Operational Security Doctrine for the FORTEZZA User PCMCIA Card*, December 1, 2001

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

[DM 3440-001](#), *USDA Classified National Security Information Program Manual*, May 1, 2008

[DR 3440-001](#), *USDA Classified National Security Information Program Manual*, October 5, 2011

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

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

[DR 4600-003](#), *USDA Insider Threat Program*, June 30, 2014

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

Federal Information Security Modernization Act of 2014 ([FISMA](#)), 44 U.S.C. § 3541, et seq.

National Institute of Standards and Technology (NIST) [Special Publication \(SP\) 800-53](#), Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, errata as of January 15, 2014

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](#), Transmittal Memorandum No. 4, *Management of Federal Information Resources*, November 28, 2000