



governmentattic.org

"Rummaging in the government's attic"

Description of document: Federal Energy Regulatory Commission (FERC)'s policy on sensitive information embodied in two records: Information Governance Policy and Guidelines for the Protection of Sensitive Information, 2016

Requested date: 23-January-2017

Released date: 07-March-2017

Posted date: 27-March-2017

Source of document: Freedom of Information Act Request
Federal Energy Regulatory Commission
Office of External Affairs
888 First Street, NE
Washington, DC 20426
Fax: 202-208-2106
Email: foia-ceii@ferc.gov
[FERC Electronic FOIA Request Form](#)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

MAR 7 - 2017

Re: FOIA No. FY17-32,
Response Letter

ELECTRONIC AND REGULAR MAIL

This is a response to your correspondence received on January 23, 2017, in which you requested information pursuant to the Freedom of Information Act (FOIA)¹, and the Federal Energy Regulatory Commission's (Commission) FOIA regulations, 18 C.F.R. § 388.108 (2016). Specifically, you requested a copy of FERC's policy on sensitive information found at a particular link referenced in your request. A search of the Commission's non-public files identified two (2) responsive documents, which are being released in their entirety. The documents are enclosed.

As provided by the FOIA and 18 C.F.R. §388.110(a)(1) of the Commission's regulations, any appeal from this determination must be filed within 90 days of the date of this letter. The appeal must be in writing, addressed to David L. Morenoff, General Counsel, Federal Energy Regulatory Commission, 888 First Street, NE, Washington, D.C., 20426, and clearly marked "Freedom of Information Act Appeal." Please include a copy to Charles A. Beamon, Associate General Counsel, General and Administrative Law, at the same address.

You also have the right to seek dispute resolution services from the FOIA Public Liaison of the agency or the Office of Government Information Services (OGIS). Using OGIS services does not affect your right to pursue your appeal. You may contact OGIS by mail at Office of Government Information Services, National Archives and Records

¹ 5 U.S.C. § 552, *as amended* by the FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 (2016).

Administration, Room 2510, 8601 Adelphi Road, College Park, MD 20740-6001; email at ogis@nara.gov; telephone at 301-837-1996; facsimile at 301-837-0348; or toll-free at 1-877-684-6448.

Sincerely,

A handwritten signature in cursive script that reads "Leonard M. Tao". The signature is written in dark ink and is positioned to the right of the word "Sincerely,".

Leonard M. Tao
Director
Office of External Affairs

Enclosures

CUI

Federal Energy Regulatory Commission

Information Governance Policy



May 30, 2016

Federal Energy Regulatory Commission
Information Security and Systems Assurance Division
888 1st Street NE
Washington, DC 20426

Document Control

This is a controlled document produced by the Federal Energy Regulatory Commission. The control and release of this document is the responsibility of the document owner. This includes any amendment that may be required.

Document Control	
Date	May 30, 2016
Author	Jeremy Barker
Document Title	Information Governance Policy

Owner Details	
Name	Anton Porter
Office/Region	Federal Energy Regulatory Commission, Washington, DC 20426
Contact Number	(202) 502-8728
E-mail Address	Anton.Porter@ferc.gov

Revision History			
Issue	Date	Author(s)	Comments
1.0	5/30/16	Jeremy Barker	Initial Release

Contents

1. Introduction.....	1
1.1 Authority	1
1.2 Purpose.....	1
1.3 Background	1
1.4 Scope.....	1
2. Policy	2
3. Key Roles and Responsibilities	3
Summary Table of key roles	3
Appendix A: Acronyms and Definitions	5
Appendix B: APPROVAL.....	6

1. INTRODUCTION

1.1 Authority

Applicable Executive Orders, national policy, and public laws for this policy include the following:

- OMB M-06-16: Protection of Sensitive Agency Information
- NIST 800-14: Principles and Practices for Securing IT Systems
- NIST 800-53: Recommended Security Controls for Federal Information Systems and Organizations
- Executive Order 13526, “Classified National Security Information.”
- Executive Order 13556, “Controlled Unclassified Information.”
- Draft 32 CFR Part 2002 “Controlled Unclassified Information”
- Managing Government Records Directive (M-12-18)

1.2 Purpose

This document provides policy governing the manner in which Federal Energy Regulatory Commission (heretofore referred to as FERC or Commission) and contractor employees manage controlled unclassified information (CUI) and Classified National Security Information (CNSI). This policy does not supersede any other applicable law.

1.3 Background

This policy establishes new guidelines and additional responsibilities for employees at FERC. It establishes the roles, responsibilities and rules of behavior with regard to handling information at FERC.

The companion manual to this policy, the FERC Guidelines for the Protection of Sensitive Information, describes in detail the fundamental procedures critical for identifying, marking, protecting, disseminating, and decontrolling FERC Controlled Unclassified Information and FERC Classified National Security Information.

1.4 Scope

This policy applies to all documents that are handled by FERC employees in the pursuit of official Commission business.

2. POLICY

All FERC documents must adhere to the guidelines below:

1. All Commission documents shall be designated, marked, safeguarded, and decontrolled in accordance with the provisions of the FERC Guidelines for the Protection of Sensitive Information.
2. Information created or handled at FERC that is deemed to potentially pose a threat to national security (e.g. Confidential, Secret, or Top Secret) and is not marked accordingly should immediately be reported to the Security and Safety Division (SAS_securityandsafety@ferc.gov), who will consult the Department of Energy's Classification Department for proper designation.
3. Commission information shall be designated in accordance with the Guidelines for the Protection of Sensitive Information.
4. All Commission employees and contractors must label or mark each document containing Sensitive CUI with its appropriate label and must undergo training on these policies every two years.
5. Information Stewards will be identified for each Office who will provide guidance and oversight to employees to ensure the Information Governance Policy is followed.
6. A CUI Senior Agency Official (CUI SAO) will be identified as having the authority to designate information as Sensitive CUI.
7. Documents may be decontrolled when the label is no longer applicable.
8. All documents deemed as records shall be maintained in accordance with FERC Comprehensive Records Disposition Schedules and General Records Schedules which provide mandatory retention requirements. The unlawful removal from the Commission of Agency records, as well as the unlawful destruction of Agency records, is a crime.
9. Upon departing service at the Commission, a departing employee may not remove or disclose classified information or Sensitive CUI.
10. Failure to comply with this policy may be a violation of the terms imposed by the Rules of Behavior pertaining to FERC activities and Federal Law and may lead to civil, administrative, and/or criminal sanctions. Such noncompliance shall be immediately reported to the Security and Safety Division (SAS_securityandsafety@ferc.gov) and/or the Chief Information Security Officer (InformationGovernance@ferc.gov) for review and investigation, as appropriate.

3. KEY ROLES AND RESPONSIBILITIES

Individuals at FERC may be designated as one or more of the following roles and will be responsible for upholding certain responsibilities outlined in the table below.

Summary Table of key roles

Role	Primary Responsibilities
Agency Head	Ensure agency senior leadership support, and make adequate resources available to implement, manage, and comply with the CUI Program as administered by the NARA's Information Security Oversight Office (ISOO).
Chief Information Officer (CIO)	Responsible for ensuring that the Commission implements and complies with applicable statutes, regulations and policy with regards to the Information Governance Program. Ensures that periodic evaluations of the Information Governance/CUI program are performed and that noted deficiencies are addressed and resolved.
CUI Senior Agency Official (CUI SAO)	Responsible to the agency head for implementation of the CUI Program within the Commission. Serves as the Designation Authority (DA). The CUI Senior Agency Official must also be the primary point of contact for official correspondence, accountability reporting, and other matters of record between the Commission and NARA's Information Security Oversight Office (ISOO).
Chief Information Security Officer (CISO)	Establish and enforce Information Governance Policy controls. Provide technical expertise and evaluate the effectiveness of Information Governance Policy. Ensure users have the appropriate level of clearance prior to being granted access to sensitive IT resources.
Information Governance Board (IG Board)	Refines the overall mission and goals of the information governance program. Defines, documents, and communicates information governance policies to key constituents. This board will consist of the CIO, CUI SAO, and Information Stewards.

Role	Primary Responsibilities
Information Steward	<p>Enforces activities to ensure adherence with information governance policies.</p> <p>Analyze compliance with policies and make recommendations for improvement of Information Governance.</p> <p>Provides recommendations to CUI Senior Agency Official on proper designations for information.</p> <p>Authorizes the timelines and events for the decontrol of information under their purview.</p> <p>At least one Information Steward must be appointed for each Office.</p>
CUI Program Manager	<p>Responsible for managing matters related to the day-to-day operations of the Commission's Information Governance/CUI program.</p>
Classification Advisory Officer	<p>Serves as the Classification Advisory Officer for all classification determinations. The Classification Advisory Officer is the primary point of contact for official correspondence, accountability reporting, and other matters of record between the Commission and Department of Energy.</p>
Document Owner	<p>Responsible for ensuring the proper marking exists on documents under their purview. Though documents may have multiple authors, the document owner provides guidance to authors on what marking is appropriate.</p> <p>Responsible for determining whether documents may be decontrolled, based on applicable law, regulation, or guideline.</p>

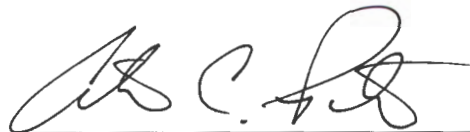
APPENDIX A: ACRONYMS AND DEFINITIONS

Acronym/Term	Definition
C.F.R.	Code of Federal Regulations
CIO	Chief Information Office
CISO	Chief Information Security Officer
CUI	Controlled Unclassified Information:
Decontrol	Decontrol is the action of removing safeguarding or dissemination controls from CUI that no longer requires them.
Designation	Designation is the determination by an authorized holder that a specific item of information is included in a CUI category or subcategory and the consequent marking of that information as CUI.
DA	Designation Authority
Dissemination	Dissemination includes transmitting, transferring, or providing access to CUI between authorized holders through any means.
Document	“Documents” refers to any written information used to conduct official FERC business, including but not limited to Word documents, Excel, PowerPoint, emails, written notes, etc.
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
ISOO	Information Security Oversight Office
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SAO	Senior Agency Official
Sensitive CUI	Certain categories of CUI at FERC has been identified as “Sensitive CUI” and requires particular labelling and handling guidelines. These are identified in the Guidelines for the Protection of Sensitive Information.

APPENDIX B: APPROVAL

I hereby approve the implementation of this Information Governance Policy. This Policy will become effective on 5/30/16
Date

Signature:



Date:

5/30/16

Anton Porter
Executive Director

CUI

Federal Energy Regulatory Commission

Guidelines for the Protection of Sensitive Information



May 30, 2016

Federal Energy Regulatory Commission
Information Security and Systems Assurance Division
888 1st Street NE
Washington, DC 20426

Document Control

This is a controlled document produced by the Federal Energy Regulatory Commission. The control and release of this document is the responsibility of the document owner. This includes any amendment that may be required.

Document Control	
Date	May 30, 2016
Author	Jeremy Barker
Document Title	Guidelines for the Protection of Sensitive Information

Owner Details	
Name	Anton Porter
Office/Region	Federal Energy Regulatory Commission, Washington, DC 20426
Contact Number	(202) 502-8728
E-mail Address	Anton.Porter@ferc.gov

Revision History			
Issue	Date	Author	Comments
1.0	05/30/2016	Jeremy Barker	Initial Release

Table of Contents

1. Introduction.....	4
1.1 Authority	4
1.2 Purpose.....	4
1.3 Scope.....	4
2.0 Classified Information	5
2.1 Criteria for Determining Classified Information	5
2.2 Handling Classified Information.....	5
3.0 Unclassified Information	6
3.1 FERC Sensitive Controlled Unclassified Information.....	6
3.2 Other Information not intended for Public Release	7
4.0 Handling Guidelines for Sensitive CUI	8
4.1 Marking and Labelling FERC-generated Sensitive CUI	8
4.1.1. Marking FERC Documents with multiple Sensitive CUI Categories	9
4.1.2 Marking Information Created in Non-Standard Formats.....	9
4.1.3 Marking and Labelling Information Created Outside of FERC	9
4.2 Storing and Accessing Information at FERC.....	10
4.2.1 Electronic Storage.....	10
4.2.2 Hardcopy Documents.....	10
4.2.3 Portable Digital Media Storage.....	11
4.3 Disseminating Information	12
4.3.1 Disseminating Information to FERC employees and Contractors (Internal).....	12
4.3.2 Disseminating Information to non-FERC employees (External).....	12
4.3.3 Disseminating Information to government agencies	12
4.3.4 Use of CUI from External Sources in FERC created material	12
4.4 Decontrolling and Destroying Sensitive CUI	13
4.5 CUI received from External Sources	14
4.6 Lost or Stolen Sensitive CUI	14
4.7 Exceptions.....	14
Appendix A: Condensed Table of Controlled Information Types.....	15
Appendix B: Marking and Labelling Requirements	17
Appendix C: Storage Requirements.....	18
Appendix D: Dissemination Requirements [Internal FERC Use]	19
Appendix E: Dissemination Requirements [External to FERC].....	20
Appendix F: Decontrol and Destruction Requirements.....	21
Appendix G: Acronyms and Definitions	22

1. INTRODUCTION

1.1 Authority

Applicable Executive Orders, national policy, and public laws for this policy include the following:

- OMB M-06-16: Protection of Sensitive Agency Information
- FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems
- FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems
- Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- Special Publication 800-60, Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories
- Executive Order 13526: Classified National Security Information
- Executive Order 13556: Controlled Unclassified Information
- Department of Energy Order 470.4B Safeguards and Security Program
- NIST Special Publication 800-171 (Final Public Draft) Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

1.2 Purpose

This document is a guideline for (a) how to determine whether a protected status should be applied to information and (b) how to handle certain types of protected information. This document supplements the FERC Information Governance Policy.

1.3 Scope

These guidelines apply to all documents created or handled by FERC employees and contractors. “Documents” refers to any written information used to conduct official FERC business, including but not limited to Word documents, Excel, PowerPoint, emails, written notes, etc.

2.0 CLASSIFIED INFORMATION

There are three levels of classification identified in Executive Order 13526 (Classified National Security Information): Confidential, Secret, and Top Secret Information. Only authorized personnel may access and handle classified information and must have the appropriate clearance to do so. A small subset of FERC employees has this authorization, and this information is managed by Security and Safety (SAS) Division.

2.1 Criteria for Determining Classified Information

Information can only be classified at those three levels if it meets all of the criteria for original classification found in E.O. 13526 Section 1.1, which are:

1. an original classification authority is classifying the information.
2. the information is owned by, produced by or for, or is under the control of the United States Government.
3. the information falls within one or more of the categories of information listed in section 1.4 of this order; and
4. the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the original classification authority is able to identify and describe the damage.

If the information does not meet all of the criteria for classification under Section 1.1 of E.O. 13526, it cannot be classified and is considered Unclassified Information.

2.2 Handling Classified Information

Only authorized personnel with the appropriate US government clearance level may handle classified information. If any FERC employees come across classified information and they are not authorized to view it, or have knowledge of classified information that is improperly handled, they must contact the Security and Safety Division immediately (SAS_securityandsafety@ferc.gov).

All authorized personnel are required to consult the Security and Safety Division prior to reproducing, disseminating, or destroying classified materials.

3.0 UNCLASSIFIED INFORMATION

The federal government identifies two main categories for unclassified information: Unclassified and Controlled Unclassified Information (CUI). “Unclassified” applies to information that does not meet the criteria for any of the classification levels listed in **Section 2.1** (Confidential, Secret, or Top Secret). This includes information to which additional protection mechanisms are not applied. Unclassified documents that do not fit the criteria for CUI may be considered “Public.”

The other category, CUI, is for information that 1) does not meet the criteria for any of the levels of classification as stated in E.O. 13526 but 2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

3.1 FERC Sensitive Controlled Unclassified Information

Certain CUI at FERC has been identified as “Sensitive CUI” and requires particular labelling and handling guidelines. Any information that could be considered Sensitive CUI shall be labelled and handled per the guidelines described in **Section 4** and **Appendices B – F**. In cases where FERC-generated information does not fit any of the descriptions in **Section 3.1**, but that may be deemed appropriate for additional protections, the office’s Information Steward shall be consulted.

The following table lists the Sensitive CUI categories used at FERC.

CUI Category	Definition
Critical Energy Infrastructure Information (CEII)	Engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: a) Relates details about the production, generation, transportation, transmission, or distribution of energy; b) could be useful to a person in planning an attack on critical infrastructure; c) is exempt from mandatory disclosure under the FOIA, and d) does not simply give the general location of the critical infrastructure. 18 C.F.R. 388.113
Information Systems Vulnerability Information	Related to information that if not protected, could result in adverse effects to information systems. Information system means a discreet set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Law Enforcement/ Investigation	Law Enforcement: Related to techniques and procedures for law enforcement operations, investigations, prosecutions, or enforcement actions. Investigation: Related to information obtained during the course of a law enforcement investigation.
Privacy*	Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-07-16, or "means of identification" as defined in 18 USC 1028(d)(7). No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

CUI Category	Definition
Privileged	Denotes information that Commission and judicial precedent recognizes as confidential, including certain submissions by the public and certain information created or compiled by FERC staff.
Procurement Sensitive	Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.
Source Selection Sensitive	Per FAR 2.101: any of the following [sic] information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly.
Transportation// Sensitive Security Information (SSI)	<p>Transportation: Related to any mode of travel or conveyance by air, land, or waterway.</p> <p>SSI: As defined in 49 C.F.R. Part 15.5, Sensitive Security Information is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DOT has determined would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to transportation safety. As defined in 49 C.F.R. Part 1520.5, Sensitive Security Information is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DHS/TSA has determined would, among other things, be detrimental to the security of transportation.</p>

*Privacy is a label used when personal information is present in a document. Personally Identifiable Information (PII) is a subset Privacy information that refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. More specific procedures for handling PII are detailed in the "Procedures on Handling FERC-Controlled Personally Identifiable Information."

3.2 Other Information not intended for Public Release

Some information that FERC produces or handles may not meet the criteria for Sensitive CUI defined in **Section 3.1**, yet still not be intended for public release. Such information may have a variety of labels, such as "For Official Use Only," "Non-Public," "Controlled," and others. If one of these labels is present on the document, but does not match one of the Sensitive CUI labels as outlined in **Appendix B**, employees are encouraged to take additional care when handling this information.

4.0 HANDLING GUIDELINES FOR SENSITIVE CUI

This section provides guidance on proper handling procedures for documents so that they are protected from unauthorized access. “Handling” refers to manipulating information or data, including, but not limited to: creation, labelling (marking), electronic transmission (emailing, faxing, scanning, sending by mail), hardcopy transmission (mail or courier), storage (electronic or hard copy), archiving, and reproduction (printing).

“Authorized holder” is a term used to distinguish who is allowed access to certain information. Authorized holders may include people outside the Commission who have a lawful Government purpose to have, transport, store, use, or process CUI, but also include people within the Commission who must handle, process, store, or maintain CUI in the course of their jobs. Commission employees must therefore use discretion to determine who is an authorized holder within the context of their mission and governing authorities. In some cases, written notices may exist that provides more explicit guidance on who may be authorized holders to certain types of information.

If an employee is ever unsure as to whether a potential recipient of information is authorized to view it, they should consult their Information Steward for clarification.

4.1 Marking and Labelling FERC-generated Sensitive CUI

The following marking and labelling requirements apply to all FERC Sensitive CUI:

- All documents created by FERC employees or contractors that contain Sensitive CUI must be labeled.
- All labels must be *prominently displayed* on each page of the document (preferably on the *top center* of the document). Examples of document labels are provided below.

CUI Category	Header Labels
Information Systems Vulnerability Information	- CUI/Information Systems Vulnerability Information - CUI/ISVI
Law Enforcement// Investigation	CUI/Investigation
Critical Energy Infrastructure Information (CEII)	- CUI/Critical Energy Infrastructure Information - CUI/CEII
Privacy	- CUI/Privacy

- When multiple CUI types are present in a document, a cover page must be used that displays each CUI label. (see **Section 4.1.1**)

See **Appendix B** for the complete set of Marking and Labelling Requirements.

4.1.1. Marking FERC Documents with multiple Sensitive CUI Categories

When a document contains multiple categories of Sensitive CUI, the document must have a cover page that is clearly labeled with each of the CUI categories contained within the document. This cover page itself should not display any sensitive material. The Sensitive CUI categories should be listed in alphabetical order and be prominently displayed on each subsequent page. The document must be handled in accordance with the Sensitive CUI type that has the most restrictive handling requirements.

4.1.2 Marking Information Created in Non-Standard Formats

Some Sensitive CUI material is generated in formats that do not lend themselves to traditional marking or labelling methods. This may apply to such difficult to label file formats such as .jpg, .wmv, .wav, .csv, and others. Staff are encouraged to mark this material where possible. If this material is not able to be marked, it must still be handled according to the guidelines of its respective data category, particularly when disseminating.

4.1.3 Marking and Labelling Information Created Outside of FERC

Documents that are unchanged when received from an outside entity (government or non-government) do not need to be re-labelled when received by FERC. However, any such documents received by FERC must be handled in accordance with its information type as defined in **Appendices C-F**.

4.2 Storing and Accessing Information at FERC

Once a document is created or received by FERC, it is the responsibility of the employee to ensure that it is stored appropriately and that access is granted only to those authorized to view it.

4.2.1 Electronic Storage

Electronic Storage refers to files that are located in a FERC-owned information system. Examples of these systems include: the FERC file system (personal and shared directories), email, SharePoint, SharePoint Online, laptop hard drives, and other non-public systems that are available only to FERC employees. Access to Sensitive CUI should only be granted to those authorized to use it. In some cases, there may be additional access requirements.

See **Appendix C** for a detailed list of requirements.

4.2.2 Hardcopy Documents

“Hardcopy documents” refers to printed or hand-written materials. All hardcopy Sensitive CUI must be safeguarded to prevent unauthorized disclosure. Unless it is needed to conduct FERC business, hardcopy Sensitive CUI should not leave official FERC buildings. Privacy CUI should not leave official FERC buildings under any circumstances. Sensitive CUI should not be printed outside of FERC official buildings. Official FERC buildings include the FERC DC offices at 888 and 1100 First Street NE, as well as the Regional Offices at New York, Atlanta, Chicago, Portland, and San Francisco.

Certain Sensitive CUI types may have additional restrictions regarding hardcopy storage. For example, certain Sensitive CUI documents are required to be kept in locked or access-controlled rooms within FERC buildings when they are not actively being used.

See **Appendix C** for a detailed list of storage requirements for each Sensitive CUI type.

4.2.2.1 Telework Guidance for Hardcopy Storage

These Guidelines apply to employees when teleworking. Employees typically telework at their Alternate Worksite as established in their FERC Telework Agreement, which is defined as a “place away from the Official Worksite that has been approved for the performance of assigned official duties.” FERC Telework Policy states that each employee is responsible to “maintain a proper and appropriate working environment at the Alternate Worksite.”

As stated in the previous section (Section 4.2.2), Sensitive CUI should not leave official FERC buildings unless it is needed to conduct FERC business. Privacy CUI should not leave official FERC buildings under any circumstances. Sensitive CUI of any category should not be printed at an employee’s Alternate Worksite.

In cases where Sensitive CUI must be brought to an employee’s Alternate Worksite in order to conduct FERC business, reasonable care must be exercised with the material to ensure that it is not easily accessible or visible to individuals not authorized to view it. The following precautions should be taken when working with Sensitive CUI at the Alternate Worksite:

- Sensitive CUI should not be plainly visible when unattended.

- When possible, Sensitive CUI should be kept in a locked container when not actively used.
- Sensitive CUI should be brought back to an official work building when no longer required for use outside of the office.

Under any circumstances, Sensitive CUI that is lost or stolen must immediately be reported to IT Support (it-support-center@ferc.gov).

4.2.2.2 Guidance for Transporting and Travelling with Sensitive CUI

When transporting Sensitive CUI, reasonable care must be exercised with the material to ensure that it is not easily accessible or visible to individuals not authorized to view it. The following precautions should be taken:

- Keep Sensitive CUI out of plain view – store material in a bag, folder, or other container to keep out of plain sight.
- If possible, keep material in locked container, such as briefcase or safe.
- Ensure that you are aware of the location of Sensitive CUI at all times.
- If travelling via air or train, it is preferable to keep Sensitive CUI with carry-on luggage, rather than checking it where it can more easily be lost.
- If transporting Sensitive CUI in an automobile, keep the material out of plain view (preferably in trunk or glove compartment) and ensure your doors are locked. Sensitive CUI should not be kept unattended in your car for an extended period of time.
- When staying in a hotel or working at a location other than your Alternate Worksite as required for FERC business, exercise precautions as outlined in the previous section (Section 4.2.2.1).

Under any circumstances, Sensitive CUI that is lost or stolen must immediately be reported to IT Support (it-support-center@ferc.gov).

4.2.3 Portable Digital Media Storage

Portable digital media refers to all forms of data within the following categories: (a) Digital media (e.g., magnetic tapes, external/removable hard drives, flash/thumb drives, compact discs, digital video disks), and (b) Portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). The following minimum restriction applies to Sensitive CUI stored in FERC-issued portable digital media.

- Digital media with Sensitive CUI must be encrypted and use FIPS validated encryption that meets the FERC User Password Policy.

4.3 Disseminating Information

Information dissemination refers to sending or providing access to information. Information can be transmitted through multiple means, including, but not limited to: electronic or postal mail, applications (e-Filing, e-Library, etc.), or simply exchanged by hand.

Access requirements must be complied with when information is disseminated, whether internally or externally to FERC. Under no circumstances can a FERC employee knowingly provide Sensitive CUI to individuals who are not authorized to view it. If an employee is ever unsure as to whether a potential recipient of information is authorized to receive it, they should consult their Information Steward for clarification.

4.3.1 Disseminating Information to FERC employees and Contractors (Internal)

Most Sensitive CUI can be sent to authorized FERC employees with minimal restrictions, though certain Sensitive CUI types have greater restrictions than others. See **Appendix D** for a detailed list of requirements for each CUI type.

4.3.2 Disseminating Information to non-FERC employees (External)

FERC employees must take extra precautions when disseminating Sensitive CUI to individuals or entities outside of FERC. When sharing Sensitive CUI with external non-governmental parties, FERC must have an existing agreement in place that authorizes information-sharing with the party. These agreements include a requirement that all parties, federal and non-federal, comply with the same standards as agencies when handling, storing, or using Sensitive CUI obtained through the agreement.

In most cases, a Memorandum of Understanding (MOU) or Non-Disclosure Agreement (NDA) will serve as the written agreement to all FERC to provide CUI to non-FERC employees. These agreements are facilitated by the Office of the Executive Director (OED), and the Office of General Counsel (OGC). Furthermore, Sensitive CUI material must be properly protected and/or labelled while in transit to further identify and safeguard it. See **Appendix E** for a detailed list of requirements for each CUI type.

Contact the office Information Steward for further guidance when considering providing Sensitive CUI to individuals or entities outside of FERC when written agreements are not yet in place.

4.3.3 Disseminating Information to government agencies

Sensitive CUI should be freely exchanged amongst other federal agencies as long as its dissemination furthers a lawful Government purpose. A written agreement is only necessary when establishing a perpetual connection or if there is a regulation that requires it. In all cases, requirements outlined in **Appendix E** must be adhered to for each CUI type.

4.3.4 Use of CUI from External Sources in FERC created material

Any FERC documents that are created with information provided by an external source (government or non-government) must be appropriately marked and handled in accordance with

both FERC Information Governance Policy as well as guidance from the other government agency or non-government source.

4.4 Decontrolling and Destroying Sensitive CUI

Decontrol is the action of removing safeguards or dissemination controls from Sensitive CUI that no longer requires them. Certain events that necessarily bring Sensitive CUI documents into the public forum automatically decontrol these documents. Examples of such events include, but are not limited to, their mention in a public Commission issuance, public release through Freedom of Information Act (FOIA) request, and use in litigation or administrative proceedings.

When feasible, Sensitive CUI, should include a specific date or event for decontrol. This only pertains when a specific date or event is known that will conclude the documents' need for additional protections. For example, a cover sheet or header on CUI budget information prepared for FY2011 may indicate that the information becomes public after October 1, 2021.

Destruction refers to deleting electronic files and shredding physical media. All physical media that contains Sensitive CUI must be placed into an approved shredding bin when it is no longer needed, except when it is appropriate for reuse (such as in the case of encrypted thumb drives).

Note that all documents, including Sensitive CUI, shall be maintained in accordance with FERC Comprehensive Records Disposition Schedules and General Records Schedules which provide mandatory retention requirements.

4.5 CUI received from External Sources

Any CUI received from sources external to FERC that fall into one of the Sensitive CUI categories listed in **Appendix A**, must be handled according to the guidelines provided in this document.

FERC may receive documents from outside sources (government and non-Government) that have different CUI labels or that request “controlled” treatment of that information in order to limit its access, without specifying its handling guidelines. If FERC receives CUI with a label not commonly used at FERC, it is the responsibility of the FERC employee who received the document to request and follow guidance from the sender prior to using or disseminating the information.

4.6 Lost or Stolen Sensitive CUI

Under any circumstances, Sensitive CUI that is lost or stolen must immediately reported to IT Support (it-support-center@ferc.gov).

4.7 Exceptions

Certain situations, such as FOIA requests, investigative actions, or other legally binding actions may trigger a change in how Sensitive CUI is protected or handled. These situations should be handled on a case-by-case basis and only by certain individuals who are formally designated authority to do so by FERC.

Notwithstanding the above, permanent deviations or temporary waivers can be granted in cases where it is not possible to conform to the minimum requirements as described in this document. These can be due to physical, technological, or other circumstantial reasons. In order to request an exemption from the requirements located in this document, FERC employees may contact their Information Steward. Information Stewards may reach out to the IT Security group (InformationGovernance@ferc.gov) for assistance, if necessary.

APPENDIX A: CONDENSED TABLE OF CONTROLLED INFORMATION TYPES

Information Types	Definition
Classified	
Top Secret	Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally <i>grave damage</i> to the national security that the original classification authority is able to identify or describe.
Secret	Information, the unauthorized disclosure of which reasonably could be expected to cause <i>serious damage</i> to the national security that the original classification authority is able to identify or describe.
Confidential	Information, the unauthorized disclosure of which reasonably could be expected to cause <i>damage</i> to the national security that the original classification authority is able to identify or describe.
Sensitive Controlled Unclassified Information (CUI)	
Critical Energy Infrastructure Information (CEII)	Engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: a) Relates details about the production, generation, transportation, transmission, or distribution of energy; b) could be useful to a person in planning an attack on critical infrastructure; c) is exempt from mandatory disclosure under the FOIA, and d) does not simply give the general location of the critical infrastructure. 18 C.F.R. 388.113
Information Systems Vulnerability Information	Related to information that if not protected, could result in adverse effects to information systems. Information system means a discreet set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Law Enforcement/ Investigation	Law Enforcement: Related to techniques and procedures for law enforcement operations, investigations, prosecutions, or enforcement actions. Investigation: Related to information obtained during the course of a law enforcement investigation.
Privacy*	Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-07-16, or "means of identification" as defined in 18 USC 1028(d)(7). No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.
Privileged	Denotes information that Commission and judicial precedent recognizes as confidential, including certain submissions by the public and certain information created or compiled by FERC staff.
Procurement Sensitive	Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.
Source Selection Sensitive	Per FAR 2.101: any of the following [sic] information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly.

Information Types	Definition
Transportation// Sensitive Security Information (SSI)	<p>Transportation: Related to any mode of travel or conveyance by air, land, or waterway.</p> <p>SSI: As defined in 49 C.F.R. Part 15.5, Sensitive Security Information is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DOT has determined would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to transportation safety. As defined in 49 C.F.R. Part 1520.5, Sensitive Security Information is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DHS/TSA has determined would, among other things, be detrimental to the security of transportation.</p>

*Privacy is a label used when personal information is present in a document. Personally Identifiable Information (PII) is a separate category of information that refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Procedures for handling PII are detailed in the "Procedures on Handling FERC-Controlled Personally Identifiable Information."

APPENDIX B: MARKING AND LABELLING REQUIREMENTS

Once a determination is made on the CUI category (left column), apply the header label. All labels must be *prominently displayed* on each page of the document (preferably on the *top center* of the document).

Sensitive CUI Category	Header Label
Critical Energy Infrastructure Information (CEII)	- CUI/ Critical Energy Infrastructure Information (CEII) - CUI/ CEII
Information Systems Vulnerability Information	- CUI/ Information Systems Vulnerability Information - CUI/ ISVI
Law Enforcement/ Investigation	- CUI/ Investigation
Privacy*	- CUI/ Privacy
Privileged	- CUI/ Privileged
Procurement Sensitive	- CUI/ Procurement Sensitive
Source Selection	- CUI/ Source Selection
Transportation// Sensitive Security Information (SSI)	- CUI/ Sensitive Security Information - CUI/ SSI
Multiple Information Types*	- CUI/ [each information type]
Other**	See note below.

* When a document contains information with multiple CUI information categories, it must contain a cover sheet that lists each of the CUI categories used in the document. This cover sheet should not contain any sensitive material.

** If FERC receives CUI with a label not commonly used at FERC, it is the responsibility of the FERC employee who received the document to request and follow guidance from the sender prior to using or disseminating the information. This does not apply to documents submitted via external filing systems, where the marking and handling instructions are specified on the systems and selected by the submitter.

APPENDIX C: STORAGE REQUIREMENTS

CUI Category	Hardcopy Storage*	Allowed portable digital media types
Critical Energy Infrastructure Information (CEII)	Access-controlled or locked room/ cabinet	Encrypted media**
Information Systems Vulnerability Information	No additional restrictions	Encrypted media
Law Enforcement/ Investigation	No additional restrictions	Encrypted media
Privacy	- Access-controlled or locked room/ cabinet - PII not allowed to leave FERC buildings	- Encrypted media - PII should not be stored on portable digital media
Privileged	Access-controlled or locked room/ cabinet	Encrypted media
Procurement Sensitive	No additional restrictions	Encrypted media
Source Selection	Access-controlled or locked room/ cabinet	Encrypted media
Transportation// Sensitive Security Information (SSI)	Access-controlled or locked room/ cabinet	Encrypted media
Other	- When receiving non-equivalent CUI from another agency, is the responsibility of the FERC employee who received the document to request and follow guidance from the sender prior to using or disseminating the information.	

* Sensitive CUI in hardcopy form that is removed from FERC premises must be safeguarded from unauthorized disclosure. This pertains to whether it is present in official FERC buildings, as well as when they are in the care of FERC employees outside of an office.

** Portable encrypted digital media refers to all forms of data within the following categories: (a) Digital media (e.g., magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks), and (b) Portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). These may be allowed with FIPS validated encryption (including PKI) that meets the NIST requirements. Contact IT Support (it-support-center@ferc.gov) for further guidance when storing CUI on digital media.

APPENDIX D: DISSEMINATION REQUIREMENTS [INTERNAL FERC USE]

CUI Category	E-Mail transfer	Transfer of hardcopy and digital media	Print
Critical Energy Infrastructure Information (CEII)	No restrictions	- Approved Courier (Signature required)** - Hand-deliver	FERC-buildings only***
Information Systems Vulnerability Information	No restrictions	- Approved Courier (Signature required) - Hand-deliver	FERC-buildings only
Law Enforcement/ Investigation	No restrictions	- Approved Courier (Signature required) - Hand-deliver	FERC-buildings only
Privacy	See note(*) below	See note(*) below	See note(*) below
Privileged	No restrictions	- Approved Courier (Signature required) - Hand-deliver	FERC-buildings only
Procurement Sensitive	No restrictions	- Approved Courier (Signature required) - Hand-deliver	FERC-buildings only
Source Selection	No restrictions	- Approved Courier (Signature required) - Hand-deliver	FERC-buildings only
Transportation// Sensitive Security Information (SSI)	No restrictions	- Approved Courier (Signature required) - Hand-deliver	FERC-buildings only
Other	When receiving non-equivalent CUI from another agency, is the responsibility of the FERC employee who received the document to request and follow guidance from the sender prior to using or disseminating the information.		
Unclassified	No requirement	No restrictions	No Restrictions

* Privacy is a label used when personal information is present in a document. Personally Identifiable Information (PII) is a separate category of information that refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Procedures for handling PII are detailed in "Handling FERC-Controlled Personally Identifiable Information."

** Approved Couriers include: USPS, FedEx, and UPS. All CUI information sent must have tracking available to ensure that it arrives at its intended destination.

*** Sensitive CUI should not be printed outside of FERC official buildings. Official FERC buildings include the FERC DC offices at 888 and 1100 First Street NE, as well as the Regional Offices at New York, Atlanta, Chicago, Portland, and San Francisco.

APPENDIX E: DISSEMINATION REQUIREMENTS [EXTERNAL TO FERC]

CUI Category	External Recipient requirements **	E-Mail transfer	Hardcopy transfer
Critical Energy Infrastructure Information (CEII)	MOU or NDA Required	- Encrypted File or Email	Approved Courier (Signature Required)
Information Systems Vulnerability Information	MOU or NDA Required	- Encrypted File or Email	Approved Courier (Signature Required)
Law Enforcement/ Investigation	MOU or NDA Required	- Encrypted File or Email	Approved Courier (Signature Required)
Privacy	Not permitted*	Not permitted	Not permitted
Privileged	MOU or NDA Required	- Encrypted File or Email	Approved Courier (Signature Required)
Procurement Sensitive	MOU or NDA Required	- Encrypted File or Email	Approved Courier (Signature Required)
Source Selection	MOU or NDA Required	- Encrypted File or Email	Approved Courier (Signature Required)
Transportation// Sensitive Security Information (SSI)	MOU or NDA Required	- Encrypted File or Email	Approved Courier (Signature Required)
Other	When receiving non-equivalent CUI from another agency, is the responsibility of the FERC employee who received the document to request and follow guidance from the sender prior to using or disseminating the information.		

* There are a very few cases in which Privacy and PII information is allowed to be transferred to parties outside of FERC, particularly to accomplish Human Resource (HR) functions or to facilitate clearance or access requests. Outside of pre-approved cases for privacy information transfer, FERC staff must contact IT Support (it-support-center@ferc.gov) and receive authorization if there is ever a perceived need to disseminate Privacy information to an external party prior to doing so.

** When providing Sensitive CUI to other US government agencies, MOUs or NDAs are not required.

*** The following forms of encryption are acceptable to use at FERC to transfer information:

1. Password encryption on file or zip folder.
2. WinZip, Entrust, and PGP Encryption Software with password.
3. Other modes of FIPS 140-2 encryption as approved by IT Security.

NOTE: All passwords used must be sent in a separate communication than the original method and meet FERC password requirements (located at <http://fercnet/newfercnet/OED/security/IT-security/policy-prod/documents/IT-User-PW-Policy.pdf>). If you need assistance disseminating highly sensitive CUI to external parties, please contact IT Support (it-support-center@ferc.gov).

**** Approved Couriers include: USPS, FedEx, and UPS. All Sensitive CUI information sent must have tracking available to ensure that it arrives at its intended destination.

APPENDIX F: DECONTROL AND DESTRUCTION REQUIREMENTS

CUI Category	Hardcopy Destruction	Decontrol
Critical Energy Infrastructure Information (CEII)	Shredding only*	Approved FOIA request only
Information Systems Vulnerability Information	Shredding only	- Event-driven** - Approved FOIA request
Law Enforcement/ Investigation	Shredding only	- Event-driven - Approved FOIA request
Privacy	Shredding only	Approved FOIA request only
Privileged	Shredding only	- Event-driven - Approved FOIA request
Procurement Sensitive	Shredding only	- Event-driven - Approved FOIA request
Source Selection Sensitive	Shredding only	- Event-driven - Approved FOIA request
Transportation// Sensitive Security Information (SSI)	Shredding only	- Event-driven - Approved FOIA request
Other	When receiving non-equivalent CUI from another agency, is the responsibility of the FERC employee who received the document to request and follow guidance from the sender prior to using or disseminating the information.	

* “Shred-It” bins are available in most areas with network printers. If a FERC-provided shredding bin is unavailable, or if you are unsure of the requirement with regards to shredding hardcopy CUI, please contact InformationGovernance@ferc.gov.

** Event-driven decontrol refers to any action, such as conclusion of legal proceeding, conclusion of investigation, or any event that makes the information no longer relevant or no longer requires consideration as CUI.

APPENDIX G: ACRONYMS AND DEFINITIONS

Acronym/Term	Definition
C.F.R	Code of Federal Regulations
CIO	Chief Information Office
CUI	Controlled Unclassified Information:
Decontrol	Decontrol is the action of removing safeguarding or dissemination controls from CUI that no longer requires them.
Designation	Designation is the determination by an authorized holder that a specific item of information is included in a CUI category or subcategory and the consequent marking of that information as CUI.
Dissemination	Dissemination includes transmitting, transferring, or providing access to CUI between authorized holders through any means.
Document Owner	Responsible for ensuring the proper marking exists on documents under their purview. Though documents may have multiple authors, the document owner provides guidance to authors on what marking is appropriate.
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
Information Steward	Role within the Commission and within each office that can provide guidance to employees on how to comply with Information Governance Policy and Guidelines.
ISOO	Information Security Oversight Office
ISSO	Information System Security Officer
NIST	NIST National Institute of Standards and Technology
OMB	OMB Office of Management and Budget
SAS	Security and Safety
Sensitive CUI	Certain categories of CUI at FERC has been identified as “Sensitive CUI” and requires particular labelling and handling guidelines. These are identified in the Guidelines for the Protection of Sensitive Information.