Federal Energy Regulatory Commission

Privacy Impact Assessment
General Support System (GSS)

Information System/Information Collection
Date Approved:
Federal Energy Regulatory Commission
Cybersecurity and Information Assurance
888 1st Street NE
Washington, DC 20426

Table of Contents

I. INTRODUCTION

In accordance with Section 208 of the E-Government Act of 2002, an agency shall complete a privacy impact assessment (PIA) when the agency develops, procures, or uses information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information in identifiable form[1] (e.g., personally identifiable information (PII)). PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual[2]. The PIA addresses privacy protections when Americans interact with the government, and it is a tool used to analyze how PII is handled to ensure that handling conforms to applicable legal, regulatory, and policy requirements as it relates to privacy. In addition, a PIA is useful in evaluating and determining privacy risks associated with the collection, processing, maintenance, use, sharing, dissemination, or disposition of information in an information system[3], information technology (IT)[4], or project/activity. Hereafter, to consolidate terminology, when the term information system is used in this document, it will apply to the meaning of an IT system and an electronic collection.

The Federal Energy Regulatory Commission (FERC) considers the PIA to be a valuable resource that provides an inventory of projects or systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. Prior to completing a PIA, FERC system owners are required to complete a Privacy Threshold Analysis (PTA). The PTA is an instrument used as the first step in the PII verification process. The PTA provides a determination as to whether a PIA is required in accordance with the E-Government Act of 2002 and allows the Commission to identify and track the types of PII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of in the Commission's information technologies, information systems, online collections or projects. A PTA is completed during the Capital Planning and Investment Control (CPIC) process. In addition, a PTA is completed when the outcome of the privacy section in the Change Request (CRQ) determines that one is required.

The Commission's PIAs must be made available to the public in accordance with the Office of Management and Budget (OMB) policy. The Commission publishes its PIAs here on FERC.gov.

[1] Information in identifiable form is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)
[2] OMB Circular NO. A-130, Managing Information as a Strategic Resource
[3] "A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." Title 44, United States Code, § 3502 (8) *Coordination of Federal Information Policy*.
[4] "Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency." See OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept 26, 2003).

II. INSTRUCTIONS

Instructions to complete this template are provided in blue font in the text boxes below. In addition, provide responses to each question in the text box below.

III. SYSTEM OVERVIEW

The General Support System (GSS) is the primary Information Technology (IT) infrastructure used by the Federal Energy Regulatory Commission (FERC) to support the daily business functions, platforms, and applications that collect, process, disseminate, and store information to support the Commission's mission.

IV. SYSTEM STATUS

1. Is this a new system or an existing system? ☐ New system ☒ Existing system

2. Is the system operated by FERC or by a contractor? ☒ FERC ☐ Contactor

3. Has a PTA been completed for this information system? ☐ Yes Provide the date.

   ☒ No

4. Does this system have a previous PIA? ☒ Yes ☐ No

   If yes, identify below the reason this PIA is being updated.

   The PIA is being updated to address the additional software, tools, and systems such as Drupal Content Manager System, Encase Endpoint Investigator, FTK Imager, Data Loss Prevention/Forcepoint Implementation, and Microsoft Azure Cloud that are a part of the GSS. Detailed information is provided for each in Section V. *Collection of PII*.

V. COLLECTION OF PII

1. Select from the table below what types of PII may be created, collected, used, maintained, disseminated, shared, disclosed, or disposed of by this information system or project.

Select all that apply.

PII TYPE	Yes
Full name	☒
Date of birth	☒
Place of birth	☒
Home address	☒
Home phone number	☒
Personal mobile phone number	☒
Personal e-mail address	☒
Passport number	☒
Driver's license/state identification numbers	☐
Financial data/financial assets (bank information (e.g., routing and account numbers))	☒
Credit card information	☒
Medical information	☐
Education records	☐
Performance appraisal	☒
Full or partial social security number (SSN)/taxpayer identification number	☒
Beneficiary information (name, home address, telephone number, SSN)	☐
Biometric data (e.g., fingerprints, iris scans, photographs)	☒
Photographic identifiers (e.g., picture, video)	☒
Age	☒
Race/ethnicity	☒
Mother's maiden name	☐
Other (Specify below)	☐

The GSS provides for the internal and external transmission and storage of Commission data. The Commission's system interconnections, various business systems and GSS software/tool and storage facility that utilize the GSS infrastructure and a description of the data used for each of the categories, where applicable, are provided below.

GSS System Interconnections

- **FERC Online (FOL)** is the single-entry point for all FERC's electronic access applications. It provides a seamless way to communicate and do business with the Commission electronically. Information collected in FOL is captured in eLibrary, recorded, and given a classification. For example, this information consists of citizen name, utility company name, and e-mail address as well as documented proceedings for which an individual is affiliated. The individual may receive notification from the Commission as it relates to these proceedings. Notification can be mailed to an individual's physical address. The FOL PIA can be accessed here.

    - **FACS (FERC Annual Charge System)** calculates and generates hydropower annual administrative and land bills as well as oil, gas, and electric bills. FERC collects annual appropriations it charges to the industries it regulates. The assessments are downloaded from the billing systems into a flat file for uploading to the Commission's core financial system (i.e.,

PeopleSoft Financials).
    - **Public Issuance Workflow (PIW)** processes and sends documents through various review steps and then publishes them to eLibrary. Documents consist of issuances which originate within the Commission and are issued by the Commission, an administrative law judge, or any other agency official with delegated authority.
    - **Virtual Agenda** provides case status information and decision documents electronically to staff throughout FERC during the stages of the Commission's deliberation process.

- **eLibrary** is a records information system that contains electronic versions of documents issued by FERC, submissions (i.e., filings) from regulated entities, and public comments (i.e., eComments). eLibrary is a publicly accessible records information system.

  The Commission releases issuances/filings (i.e., findings) on submissions. Submissions are statutory filings, which may contain sensitive business information such as Critical Energy Infrastructure Information (CEII) (e.g., dam safety information, blueprints, or dam rate information a gas pipeline may charge). In addition, eLibrary may contain law firm contact information, utility company information, forms, or documents filed by the public. Individuals also can register with eLibrary by providing full name, e-mail address, mobile phone number, and the city and state where they reside.

  The eLibrary PIA can be accessed here.

- **eForms** provides a mechanism to collect structured data from regulated entities and stores this data in a centralized database located at FERC. Categories of forms fall under electric, gas, hydropower, oil, or service companies. Structured data includes, but is not limited to, requester name, title, address and telephone number as well as the name, address and telephone number of the person or entity on whose behalf the information is requested, statement of need for electronic CEII, customers and their business addresses (top 20 purchasers of electric energy), utility fuel supply contracts, cost recovered through wholesale automatic adjustment clauses, and annual report of information detailing electric public utility officer and board of director positions that officers and directors held within and outside their affiliated public utility and during the preceding year.

- **FERC Enterprise Messaging System (FEMS2)** is a collection of applications that provides messaging services to FERC employees and contractors. It currently consists of Microsoft Office 365, a cloud-based system that provides enterprise messaging services, and Microsoft OneDrive for Business as a sharing and collaborative tool to store, sync, and share work files. Microsoft OneDrive for Business is addressed in more detail in the FEMS2 accreditation package.

  The FEMS2 PIA can be accessed here.

- **Automated Acquisition Management Solution (AAMS) (web-based application)** is an online application that provides a complete and adaptable commercial off-the-shelf acquisition process solution addressing the full acquisition lifecycle. A web-based solution provides the tools necessary to effectively manage acquisitions from initial planning to closeout.

  The AAMS PIA can be accessed here.

- **PeopleSoft Financials (web-based application)** consists of financial applications and is FERC's system of record for capturing and reporting all United States (U.S.) Standard General Ledger activity associated with appropriations, commitments, obligations, vouchers, payables, and receivables.

  The PeopleSoft Financials PIA can be accessed here.

- **The Federal Personnel and Payroll System (FPPS)** is an online personnel and payroll system providing support to the Department of the Interior (DOI) bureaus and offices, and Interior Business Center (IBC) federal agency customers. FPPS is customized to meet customer needs for creating and generating the full life cycle of personnel transactions. FPPS allows for immediate updates and edits of personnel and payroll data. FPPS also handles regulatory requirements such as specialized pay, garnishments, and special appointment programs. FPPS also operates in batch mode for performing close of business, payroll calculation, and other processes. FERC has an interconnection between FPPS and PeopleSoft Financials.

  The FPPS DOI PIA can be accessed here.

GSS Dependent Business Systems

- **Freedom of Information Act (FOIA)/**CEII Tracker 2.0 is a SharePoint-based system that allows internal staff to track the status of the FOIA/Privacy/CEII requests throughout their life cycle. The FOIA/CEII Tracker 2.0 collects contact information such as mailing addresses, names, email addresses and telephones numbers of private requestors' (i.e., individual citizens) and public requestors' (e.g., companies, organizations, federal and state agencies) received electronically by e-mail, webpage forms, regular mail or fax. The tracker collects names of the FERC Office of General Counsel, General Administrative Law (GAL) attorneys, paralegals and program office point of contacts assigned to a request. In addition, the Office of External Affairs (OEA) and GAL save CEII and Privileged materials (responsive documents to a FERC request) in the FOIA/CEII Tracker 2.0 or on restricted drives.

- **FERCollaborate (SharePoint)** is the FERC intranet SharePoint site used by the Commission program offices to easily share and collaborate on documents. This document repository is used by program offices to store various types of documents. For example, program offices upload policy materials, standard operating

procedures, guides, plans, and training. In addition, program offices store documents that are used to collect or that contain PII, such as the Chief Financial Officer country clearance form (collects employee travelers name, cell number, passport number, place of birth, and date of birth) and employee performance appraisals (contains employees' name, rating, and performance results). SharePoint site also includes draft issuances, submittals and documents containing CEII. Program office group SharePoint sites that store documents with sensitive PII or CEII provide restricted access to those employees who have an approved "need to know."

- **Office of the Administrative Law Judges** is a SharePoint application that tracks workload and procedural information surrounding the operation of the Office of Administrative Law Judges.

- **Geographic Information Systems (GIS)** is responsible for hydraulic analyses of flooding issues, developing digital elevation model data from spatial data, analyzing soil erosion, publishing maps, and enhancing geo-processing and data conversation capabilities.

- **Network** includes appliances (F5), routers, firewalls, switches, and telephone hardware.

- **Active Directory** is a directory structure used to store information and data about networks and domains. Active Directory is used to authenticate and authorize users as well as ensure that users meet FERC password standards.

- **Network Storage** is the repository of files and folders structures FERC utilizes to store business system's data. During the onboarding process, employees may store forms that contain PII to the network. Employees' may save Office of Personnel Management (OPM) Standard Form 50 Notification of Personnel Action to the network, which includes the employees' name, social security number (SSN), and date of birth. In addition, employees can also save their OPM Electronic Official Personnel Folder (eOPF) Form to the network. This document collects the employees' name, SSN, date of birth, financial and employment history data.

- **CPIC/Budget** pertains to potential and ongoing IT investments in development or in a steady state. CPIC form requested information includes, but is not limited to, the name of the FERC requestor, sponsor(s), name of office director(s), schedule, and total cost value.

- **Regional Transmission Organizations (RTOs)/Independent System Operators (ISOs)** is an ongoing data delivery from RTO and ISO of accounts and records, such as physical and virtual offers and bids, market awards, resource outputs, marginal cost estimates, shift factors, financial transmission rights, internal bilateral contracts, uplift, and interchange pricing. Data are used by FERC for marker surveillance and analysis.

GSS software, tools, and storage facility

- **Financial Disclosure Online (FDonline)** module is a cloud-based, multi-tenant, software as a service (SaaS) - that sits on the Intelliworx platform - which allows applicable government employees and ethics officers to efile and review the annual Office of Government Ethics (OGE) Form 450. The FDonline module collets the following information for the purpose of onboarding new hires and filing out financial disclosure forms. This information includes:
    - full name
    - e-mail address
    - demographics (e.g., race, nationality, ethnicity)
    - employment (e.g., work address, e-mail, grade, title, work phone)
    - Types and amounts of salaries, investments, and assets for self and spouse/family
    - Creditor names, city, state, country

- **Premisys ID software (IDenticard software)** is a security and badging package that provides the Chief Security Officer (CSO) staff with the ability to print law enforcement grade credentials for CSO special agents, CSO staff, and regional engineers. The system uses a Structured Query Language (SQL) database to store photos and signatures. The software facilitates the catering of information, the ability to retrieve it, display it and to print it.

- **Microsoft Teams** is a cloud-based team collaboration software that is part of the Office 365 suite of applications. The core capabilities in Microsoft Teams include business messaging, calling, video meetings and file sharing. It is a unified communications platform that combines persistent workplace chat, video meetings, file storage, and application integration. It also has features extensions that can integrate with non-Microsoft products.

- **F5 Secure Sockets Layer (SSL) Orchestrator (SSLO)** provides an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/Transport Layer Security (TLS) encrypted traffic. The SSLO module enables security inspection to expose threats and stop attacks. This module will decrypt all SSL traffic and store that unencrypted traffic in EnCase; a dedicated Packet Capture (PCAP) storage facility. This decrypted traffic may contain PII. However, banking, financial and health information will not be captured through the policy set.

- **Drupal Content Management System** is a content management system (CMS) with a modular design to allow features to be added and removed by installing and uninstalling modules. FERC utilizes Drupal to manage FERC.gov. Drupal modules allows FERC.gov to be able to collect information such as a user's e-mail address, username and password on its web forms.

- **Encase Endpoint Investigator** is used to collect system information from remote systems and devices for analysis and investigations. FERC utilizes Encase Endpoint to analyze information and snap images of Hard Disk Drives (HDD) and Solid-State Drive (SSD) to gather evidence.

- **FTK Imager** is a data preview and imaging tool that allows the examining of files and folders on local hard drives, network drives and CDs/DVDs. FTK Imager also allows the reviewing of the content of forensic images or memory dumps. These files may contain PII. Once the images of the files are no longer needed, they are deleted.

- **Data Loss Prevention Tool Forcepoint Implementation** is used by FERC to detect unauthorized removal of FERC data. The DLP tool collects PII during the course of scanning of Commission systems.

- **Microsoft Azure Cloud** is a cloud service for building, testing, deploying, and managing applications and services through a secure datacenter. The Azure Cloud provides software as a service (Saas), platform as service (PaaS) and infrastructure as service (IaaS). FERC uses the Azure Cloud to make a copy of data that exists in FERC on-premises databases. Data that is determined to be needed to support various projects is identified in on-premises databases and then copied to the Azure Cloud, and used for data science, business intelligence, and data visualization. PII that is copied from the FERC on-premises databases will be included in the Azure Cloud.

- **BMC Remedy** is an IT Service Management software suite used to provide easy and efficient automation of IT-related functions. FERC uses BMC Remedy to store and manage various eFiling requests and questions received from law firms, public energy utility entities, state government offices, and the public. PII stored in BMC Remedy contains individuals of the public first and last name, and personal email addresses.

2. Will the information system or project collect publicly available data? ☒ Yes ☐ No

The Commission collects publicly available data such as individuals name, email address and mailing/business address. Information collected from the public through FERC Online will be included on the GSS.

VI. AUTHORITY TO COLLECT PII

1. Provide the specific legal authorities and/or FERC regulations that permit and regulate the collection and use of PII by this information system or project?

The Commission's GSS authority to collect PII are permitted under the following legal authorities:

- Code of Federal Regulations (CFR) Title 18, Chapter I, Subchapter A, Part 3b on *Collection, Maintenance, Use, and Dissemination of Records of Identifiable Personal Information.*
- Title 31 U.S.C. §3511 *Prescribing accounting requirements and developing accounting systems*

2. Do you collect the minimum PII that is relevant and necessary to accomplish the legally authorized purpose for the collection? ☒ Yes ☐ No

The GSS collects only the minimum information necessary to administer the program.

VII. PURPOSE AND USE FOR COLLECTING PII

1. Describe the purpose and intended use for collecting, using, processing, storing, maintaining, disseminating, sharing, or disclosing the PII listed in Section V - *Collection of PII.*

The system is designed to support the general functionality of FERC. The mission of FERC is to "assist consumers in obtaining reliable, efficient, and sustainable energy services at a reasonable cost through appropriate regulatory and market means." The use of the data is relevant and necessary to support FERC's mission.

In addition, the purpose and intended use for the PII stored and maintained on the GSS is identified in Section V. *Collection of PII.*

2. Is the PII used for the sole purpose for which it was collected? ☒ Yes ☐ No

3. Who ensures that the PII is used in accordance with the purpose and reason for the collection?

The system owner assesses and ensures that the PII is used in accordance with the stated collection.

VIII. SOURCES OF PII

1. Who or what is the source(s) of the PII in this system? Select all that apply?

PII TYPE	Yes
Members of the public	☒
FERC employees	☒
FERC contractors	☒
FERC interns	☐
Federal, state, local agency	☐
Other agency employees/contractors	☐
Private sector employees	☐

United States visitors to FERC	☐
Foreign national visitors to FERC	☐
Other	☐

The information in the GSS is sourced from the above system interconnections, business dependent systems, and GSS software, tools and storage facility identified in Section V. *Collection of PII*. The systems referenced in this section obtain data from various sources, such as utility companies, private citizens, federal and state agencies, and FERC employees and contractors.

2. What method(s) is used to collect the information in this system (e.g., web form, paper form, telephone)?

   ☒ Web form ☒ Paper form ☐ Telephone ☒ Other. Please specify method below.

In addition to the above-mentioned methods for collecting information FERC utilizes CDs, DVDs and Flash drives.

3. Does another FERC information system or component send/receive PII to/from this system? ☒ Yes ☐ No

This PIA addresses FERC's GSS, which provides a central source of business system infrastructure for other system interconnections. See Section V. *Collection of PII*, for a comprehensive list of GSS interconnections, dependent systems and GSS software, tools and storage facility, and a list of data shared.

IX. CONSENT TO THE COLLECTION OF PII

1. Is the PII collected directly from the individual (e.g., member of the public and/or employee/contractor)? ☒ Yes ☐ No

2. Are individuals provided with notice prior (e.g., Privacy Act notice or link to a privacy policy) to collecting their PII? ☐ Yes ☐ No ☒ N/A

Not applicable. All information requested is statutorily required.

3. Are individuals informed that the collection of their PII is voluntary or mandatory? ☐ Yes ☐ No ☒ N/A

4. Do individuals have the opportunity to decline to provide their PII, opt out, or to consent to particular uses of their PII (other than required or authorized uses)? ☐ Yes ☐ No ☒ N/A

Not applicable. All information requested is statutorily required.

5. Are individuals informed of the consequences of not consenting to the collection of their PII?
☐ Yes ☐ No ☒ N/A

Not applicable. All information requested is statutorily required.

6. Is consent obtained from the individual prior to any new uses or disclosures of previously collected PII? ☐ Yes ☐ No ☒ N/A

X. PRIVACY NOTICES

A. System of Records Notice

1. Is the information in this information system or paper "system" (e.g., filing cabinet) **retrieved** by a personal identifier such as an individual's name, SSN, or other personal identifier? Describe below how information is retrieved.

   ☒ Yes ☐ No **Skip to section XI below.**

2. Does this system have a SORN published in the Federal Register?

   ☒ Yes. Provide SORN details below.
   ☐ No. SORN currently in development.
   ☐ No. SORN needs to be developed.

The GSS itself is not a system of records as defined in the Privacy Act of 1974, however, the GSS system interconnections and dependent business systems listed below are system of records on the GSS and both have system of records notices.

- PeopleSoft Financials (published as Management, Administrative, and Payroll System (MAPS) - FERC–56
- Commission Freedom of Information Act and Privacy Act Request Files - FERC–46

3. Is the PII contained in this information system or paper "system" used solely for the authorized purpose(s) identified in its SORN?

   ☒ Yes ☐ No ☐ SORN needs to be developed.

4. Are records in this information system or paper "system" disclosed to any person or other agency?

   ☒ Yes ☐ No

Disclosures are listed in the following SORNs:

PeopleSoft Financials (published as MAPS)

Commission Freedom of Information Act and Privacy Act Request Files

5. Is there an accounting of records kept about records disclosed to an individual or another agency? ☒ Yes ☐ No

The FERC FOIA Servicer Center (FSC) handles the accounting of disclosure of records disclosed pursuant to a Privacy Act request and the FSC and the Office of the Chief Financial Officer handles the accounting of records disclosed from PeopleSoft Financials.

6. Do you limit the collection of PII to the minimum elements identified for the purposes specified in this information system's SORN?

   ☒ Yes ☐ No

7. Is this system undergoing a modification that requires an amendment to or revision of the SORN? ☐ Yes ☒ No

8. Is the SORN for this system kept up-to-date and current?
   ☒ Yes ☐ No

Yes. The systems are kept up-to-date and current. Commission Freedom of Information Act and Privacy Act Request Files SORN was updated in 2016 and PeopleSoft Financials is currently being prepared for publication.

B. Privacy Act Statements

In addition, the Privacy Act requires federal agencies to provide what is referred to as a Privacy Act Statement to individuals prior to collecting personal information that will be contained in an agency's system of records. For example, when the Commission collects PII from an individual by web form or by paper form and this information is stored in and retrieved from a system of records, then a Privacy Act Statement is required on the form(s), along with the details about its applicable system's related SORN or on a separate form that can be retained by the individual.

9. Does this information system use an electronic or paper form to collect PII?

   ☒ Yes ☐ No **Skip to the next section.**

Yes. The FOIA-Privacy Act Request Form can be located at https://www.ferc.gov/enforcement-legal/foia/electronic-foia-privacy-act-request-form.

10. Is the PII collected by this electronic or paper form entered into this information system and retrieved by a personal identifier (e.g., an individual's name, SSN, system generated number, or another personal identifier assigned to the individual)?

☒ Yes ☐ No **Skip to the next section.**

Information in PeopleSoft Financials is retrieved by the following personal identifiers: employee's name and social security number. Information in the FOIA/PA/CEII Tracker is retrieved by the following personal identifiers: name of the individual requester, affiliation, where applicable, and subject matter.

11. Does the electronic or paper form include a Privacy Act Statement (privacy notice) notifying individuals about how their PII will be used? ☐ Yes ☒ No

12. Does this form(s) require an OMB control number? ☐ Yes ☒ No

XI. ACCESS TO PII

1. Are individuals provided the ability to have access to their PII maintained in this information system? ☒ Yes ☐ No ☐ N/A. The Privacy Act does not pertain to this system. **Skip to Question 3 below.**

2. Are there procedures in place to allow individuals access to their PII? ☒ Yes ☐ No

For PeopleSoft Financials, request from individuals to determine if a system of records contains information about them should be directed to the System Manager listed in the SORN. https://www.ferc.gov/sites/default/files/2020-05/sorn-maps.pdf For the FOIA/PA/CEII Tracker, request for access to records should be directed to the Director, Office of External Affairs. https://www.govinfo.gov/content/pkg/FR-2016-09-07/pdf/2016-21418.pdf

3. Who will have access to the PII in this information system (e.g., users, managers, system administrators, developers, contractors, third-party service providers, other)?

Users, managers, system administrators, developers, and others will have access to the data in the system.

4. How is access to the data in this information system determined?

Access varies depending on the user in question. The following FERC staff have access to the data:

- **Users**: Users such as security personnel have the business justification and access rights to the data in the system. For example, FEMS users have access to their e-mail and documents in Microsoft OneDrive for Business.
- **Managers:** Managers have access to the data as part of their assigned oversight and managerial functions. For example, specific Office of Energy Projects staff have access to CEII and privilege information in eLibrary.
- **System Administrators:** System administrators have access to the data as part of their assigned employment functions. Administrators have system access and can access other mailboxes or documents as needed.
- **Developers:** Developers have access to systems developed by FERC, e.g., FERC Online and eLibrary.
- **Other:** Each program office has their own SharePoint site. Generally, all FERC employees have access to SharePoint. However, each program office's SharePoint content manager can limit access to specific sites by item-level permissions.
- **FOIA/CEII Tracker 2.0:** The FOIA liaison and other designated OEA staff members, system administrators, GAL staff – managers, attorneys, and paralegals.
- **SharePoint:** Program offices' main FERCollaborate SharePoint sites are accessible by the entire Commission. However, there is limited access to group sites based on view, read or write access permissions.
- **FOIA/CEII Tracker 2.0:**
    - FOIA liaison and other designated OEA staff members: Read-write access
    - FOIA system administrators: Read-write access
    - GAL Attorneys: Read-only access
    - GAL paralegals: Read-write access
    - Managers: Read-only access

5. Will users have restricted access to the PII in this information system? ☒ Yes ☐ No

For most of the systems/applications, access to the data is determined by the users' role (i.e., role-based access), job function, and business justification. Access is controlled through an access control list.

SharePoint – The content manager for every site will determine permission for each program office and site. In addition, an employee can also send a ticket to the Information Technology Support Center requesting access to a specific SharePoint site. The content manager/owner of the site will determine whether to grant access.

eLibrary – Employees have access to all public files in eLibrary. When a member of the public seeks access to a document that is privileged or contains CEII, he/she must follow FERC policy as provided on ferc.gov.

FOIA/ CEII Tracker 2.0: A user's access is determined based on their role.

All documents in eLibrary are organized by library, e.g., hydropower, electric, gas, or oil. Once access to a non-public document is approved, it would be provided in hard copy.

Access to folders on a program office group SharePoint site may be restricted. To gain access, an individual must be granted permission by the content manager/owner of the site.

6. What procedures are established to limit access to only those individuals who have an "official" need to access the PII based on their role?

Standard operating procedures are in place, and privacy and security controls are documented in the risk management profile for each system/application relevant to access controls, rights and privileges.

In addition, there is a list of who has access to the FOIA/ CEII Tracker 2.0 and security assignments. There is also a handbook about how to use the system with included roles and responsibilities.

7. How is unauthorized access prevented?

The information housed in eLibrary is accessible to the public. However, based on the proprietary and sensitivity (e.g., CEII) of specific documents in eLibrary, these documents are reviewed, classified, and vetted prior to release, if at all.

The systems identified in this PIA have security access controls and role-based access controls in place to protect the data from unauthorized access or use.

Access to the data in the FOIA/CEII Tracker 2.0 is limited based on the employees' role and assigned request.

Program offices provide access restrictions to SharePoint sites where the information is sensitive and/or only those with a need to know should have access.

8. Are procedures about access controls documented? ☒ Yes ☐ No

XII. SHARING OF PII

1. Is PII shared with another federal, state, local agency, third-party (e.g., contractor/vendor), or institution?

   ☒ Yes ☐ No **Skip to question 9.**

2. Is there a formal sharing agreement in place that addresses the PII shared?

☒ Yes
☐ No **Skip to question 7.**
☐ N/A. PII is not shared outside the Commission.

3. Select the applicable sharing agreement in place.
   ☐ Confidentiality Agreement
   ☐ Non-Disclosure Agreement
   ☒ Memoranda of Understanding
   ☐ Information Sharing Agreement
   ☐ Letters of Intent
   ☒ PII is provided to, shared with, or maintained, but not by a formal sharing agreement.

PII is shared with DOI through a Memorandum of Understanding/Interconnection Security Agreement. The information that FERC shares with other federal, state, and local agencies, follows the Commission's statutes, rules, orders, and policy. PII is shared with the following: U.S. Commodity Futures Trading Commission (CFTC), Department of Energy (DOE) (U. S. Energy Information Administration (EIA), North American Electric Reliability Corporation (NERC), North American Energy Standards Board, Department of Homeland Security, Office of Management and Budget, public utility companies and state commissions, Office of Personnel Management, and U.S. Dept. of Treasury, and Department of Interior.

4. Does the sharing agreement selected above describe the purpose for sharing PII and how it will be used? ☒ Yes ☐ No

5. What privacy concerns were identified regarding the sharing of PII?

The privacy concern involved putting in place the necessary security controls to ensure the PII shared was safeguarded.

6. Who reviews and approves the agreement(s) selected above?

The Memoranda of Understanding/Interconnection Security Agreement is reviewed and updated as needed, annually by the Assessment and Authorization (A&A) team, Information Technologies Operations (ITOps) team, Human Resources (HR) and Cyber Security & Information Assurance (CsIA) team.

7. Are proposed new instances of sharing PII with third parties (e.g., contractors/vendors) evaluated to assess whether the sharing is authorized and compatible with an existing SORN?

   ☒ Yes ☐ No ☐ N/A

Yes, all new instances of sharing PII with third parties would have to be evaluated to assess whether the sharing is authorized and compatible with the FPPS SORN.

8. Are proposed new instances of sharing PII with third parties (e.g., contractors/vendors) evaluated to assess whether the sharing is authorized and in compliance with the purpose of the collection. ☒ Yes ☐ No ☐ N/A

9. Are employees trained on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII? ☒ Yes ☐ No

XIII. CLOUD SERVICE PROVIDERS/CONTRACTORS

1. Does the Commission employ a cloud service provider/contractor to operate and manage this information system? ☒ Yes ☐ No **Skip to the next section.**

2. Identify if the cloud includes Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a service (IaaS)?

- FEMS2: SaaS
- FDonline: SaaS
- Microsoft 365: SaaS
- Microsoft Azure Cloud: SaaS, PaaS, IaaS

3. Describe the data that will be collected, used, maintained, managed, or generated by the cloud service provider/contractor as part of the services under the contract.

The data in Microsoft Azure Cloud is a copy of data that exists in FERC on-premises databases. Generally, data determined to be needed to support various projects is identified in on-premises databases, copied to the Azure Cloud, and used for data science, business intelligence, and data visualization.

4. Identify the role of each individual from the cloud service provider/contractor team who will have access to the PII in this information system?

Contractors

- Admin Contractors have the ability to view the PII in the Azure Cloud as well as subset of PII from on-premises sources that have been approved by security.
- Data Modeling Contractors have the ability to view the PII information in the Azure Cloud.

5. Does the contract with this cloud service provider/contractor address who is accountable for the security and privacy of the data? ☒ Yes ☐ No

The contract addresses who is accountable for the security and privacy of the data. The core of cloud services and members of the security teams throughout CIO are held accountable for the security and privacy of the data.

6. Does the contract with this cloud service provider/contractor establish who has ownership rights over the information? ☒ Yes ☐ No

7. Does the contract with this cloud service provider/contractor address privacy roles, privacy responsibilities, and access requirements? ☒ Yes ☐ No

8. Does the contract with this cloud service provider/contractor establish record retention responsibilities for the Commission and the cloud service provider/contractor? ☒ Yes ☐ No

9. Is the acceptance of liability and incident response notifications for the exposure of PII clearly defined in the contract with the cloud service provider/contractor? ☒ Yes ☐ No

The FERC Incident Response Plan is included in the contract and details how to handle exposures of PII.

XIV. DATA QUALITY AND INTEGRITY

1. Is PII collected from members of the public or employees/contractors confirmed to be accurate, relevant, timely, and complete? ☒ Yes ☐ No

FERC collects information directly from private citizens, utility companies, business entities, employees, and federal, state and local agencies with the expectation that the information provided is accurate at the time of submission.

Information in the FOIA/ CEII Tracker 2.0 is received directly from the private or public requestor. The information is relied upon to be accurate. However, the requestor can be contacted to verify contact information.

2. Are reviews conducted to ensure that inaccurate or outdated PII contained in this system is corrected? ☒ Yes ☐ No

3. Are security controls in place to ensure the integrity of PII? ☒ Yes ☐ No

Microsoft Azure Cloud follows all the requirements under NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* for "moderate systems." The Azure Cloud uses the "Moderate" baseline rating for confidentiality and integrity, availability security objectives. The Azure Cloud enforces physical access authorizations for all physical access locations to datacenters using 24/7 security staff, alarms, video surveillance, and multifactor authentication such as Personal Identity Verification (PIV) card access.

4. Are there procedures in place to verify that the PII collected and maintained is accurate, complete, and up-to-date? ☒ Yes ☐ No

FERC relies on the information it receives from a private citizen, utility company, employee, or federal, state or local agency to be current and to notify the Commission if information submitted is inaccurate or needs to be updated. Information received from the requestor for the FOIA/ CEII Tracker 2.0 is relied on to be accurate and current. Correspondence is sent to the requestor via e-mail and regular mail in response to their request. If correspondence is sent back, the requestor is contacted and asked to provide updated information.

5. Is there a process in place for disseminating corrections or amendments of PII to external sharing partners? ☒ Yes ☐ No

6. Is PII in this information system checked for accuracy when collected from a source other than the individual to whom the information pertains?

   ☐ Yes ☐ No ☒ N/A. Not collected from another source.

XV. MONITORING, AUDITING, AND ACCOUNTABILITY

1. Is the use and sharing of PII in this information system regularly monitored to ensure that it is consistent with the authorized purpose(s) of the collection? ☒ Yes ☐ No

FERC utilizes DLP/Forcepoint solution to analyze, identify, alert, and prevent the unintentional or deliberate exfiltration of unprotected sensitive data from FERC network. One example is DLP flagging and picking up outbound emails that contain sensitive PII and preventing them from leaving. FERC also utilizes Splunk to collect and generate audit record for security-related events.

2. Are auditing procedures in place to ensure compliance with security and privacy controls?

   ☒ Yes ☐ No

3. Explain how regularly system logs are reviewed or procedures audited.

Splunk is used to detect unauthorized access and privilege access abuse in the GSS. The audit information collected is shown as a chronological record of user activities that is sufficient enough to enable the reconstruction, review, and examination of those activities. Websense is used to provide real-time content scanning and web site classification to protect

FERC computers from malicious web content while controlling employee access to dynamic, user generated web content.

FOIA/CEII Tracker 2.0: There is no capability to monitor requestors in this system. In addition, only employees who have access to a request may access the data. Audit trails capture any changes made to the data and who made the changes.

SharePoint does not provide the ability to monitor. However, a record is kept on the date and the name of who uploaded a document or made change.

4. Describe any monitoring, testing, or evaluating conducted on a regular basis to ensure the security controls and privacy controls are effective in safeguarding PII used, collected, processed, stored, maintained, disseminated, shared, or disclosed from this information system.

Access controls, audit controls, and Websense security software are used to monitor and scan Internet requests, activity logs, apply Internet usage filters, and report on activities.

Audit trails for the FOIA/ CEII Tracker 2.0 captures information about users who access the tracker and if they make updates or revisions to the data.

XVI. REDRESS

1. What is the process for receiving and responding to individuals' privacy complaints, concerns, or questions about this information system?

FOIA/Privacy/CEII tracking system: A FOIA/Privacy/CEII Request web form is filled out and submitted by the requestor. Specific contact information is required to be collected to process and respond to the requestor. However, the requestor has the option to provide his or her e-mail address if they prefer not to provide a telephone number.

PeopleSoft Financials: Privacy questions should be directed to the System Manager listed in the SORN.

In addition, on the Privacy Program website at FERC.gov, individuals are instructed to submit their privacy complaints, concerns, or questions to privacy@ferc.gov.

2. What is the process for receiving and responding to Privacy Act requests? ☐ N/A. This information system is not a system of records in accordance with the Privacy Act.

For the FOIA/Privacy/ CEII tracking system, to submit a Privacy Act request, users should complete an electronic FOIA-Privacy Act Request Form located here.

For PeopleSoft Financials, individuals should contact the System Manager listed on the SORN located here.

3. Are there procedures and a process in place to allow individuals the ability to correct or amend inaccurate or erroneous information maintained by the Commission? ☒ Yes ☐ No

For the FOIA/PA/CEII Tracker, request from individuals to correct or amend inaccurate or erroneous information should be directed to the Director, Office of External Affairs.

For PeopleSoft Financials, request from individuals to correct or amend inaccurate or erroneous information about them should be directed to the System Manager listed in the SORN.

XVII. DATA RETENTION AND DISPOSAL

1. What are the Commission's records schedule(s) or General Records Schedules (GRS) for this information system?

GSS: Due to the length of the GSS records retention schedules, the following link has been provided. https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2016-0002_sf115.pdf.

For those individuals external (i.e., outside the Commission) to FERC who would like access to the GSS records retention schedule, please visit the FERC Public Reference Room located at Room 2-A, 888 First Street, N.E., Washington, D.C. 20426. The following link has been provided for more details.

https://www.ferc.gov/public-reference-room

FOIA/CEII Tracker 2.0: Information access. protection tracking, and control records, which includes:

- records documenting receipt, internal routing, dispatch, and destruction of unclassified records;
- tracking databases and other records used to manage overall program; *and*
- requests and authorizations for individuals to have access to classified files.

2. Has the records schedule(s) been approved by the National Archives and Records Administration (NARA)? ☒ Yes ☐ No

3. What are the disposition schedules and procedures for the disposition of records containing PII at the end of the retention period?

Disposition Authority: DAA-GRS-2016-0002

Disposition Instructions: Destroy two years after last form entry, reply, or submission; or when associated documents are declassified or destroyed; or when authorization expires; whichever is appropriate. Longer retention is authorized if required for business use.

XVIII. PRIVACY AWARENESS AND TRAINING

1. Are employees/contractors who have access to this information system taken the mandatory annual FERC IT Security & Privacy Awareness training? ☒ Yes ☐ No

XIX. SECURITY AND PRIVACY SAFEGUARDS

1. What administrative procedures, technical, and physical safeguards/controls are in place to protect the PII in this information system?

All users with access to the Commission's network are required to complete an annual cybersecurity and privacy training which includes the handling of sensitive PII. In addition to training, the Commission uses the DLP/Forcepoint tool to monitor and flag the unauthorized sharing of PII outside of the Commission's network by employees.
For most of the systems/applications, access to the data is determined by the users' role (i.e., role-based access), job function, and business justification. Access is controlled through an access control list.

For employees to be given access to Commission systems they are first required to read the "Rules of Behavior for Users of Information Technology" or "Rules of Behavior for Privileged Users." Once the employee reads the above documents they are required to sign "Acknowledgement of Rules of Behavior for IT Users" in order to gain access.

2. Has this information system received an Authorization to Operate (ATO)?

The GSS will be reauthorized on March 30, 2021.

3. What privacy risks are associated with this information system and how are those risks mitigated?

The main privacy risk with any system is unauthorized access. Unauthorized access could lead to identity theft, financial fraud, and loss of public trust. These risks are mitigated by following strict access control policies based on principle of least privilege required to conduct job function.

FERC also deploys various tools to mitigate privacy risk such as the DLP/Forcepoint tool, Splunk, and Encase Endpoint Investigator.

4. Is "live data" (e.g., PII) used from this information system for testing, training, or research? ☐ Yes ☒ No

5. Does this information system use technologies and system capabilities that automate privacy controls?

Yes. FERC uses data tags to automate tracking of PII across FERC's systems' information lifecycle.

6. Provide a general description of the technologies used to protect the PII in this information system.

All data is encrypted in transit and at rest. FERC utilizes virtual private networks (VPNs) to secure the network and also utilizes Homeland Security Presidential Directive (HSPD)-12 PIV cards to add another layer of protection with two factor authentications.

XX. WEBSITE PRIVACY

1. Does this information system use a website to communicate with the public?
   ☒ Yes ☐ No **Skip to question 4.**

2. Does the website collect PII from the public? ☒ Yes ☐ No

FERC Online is a suite of integrated web-based and desktop thick-client applications that is the user interface for the submission of electronic documents by the public to FERC. FERC Online is housed in the GSS. Access the FERC Online PIA here for a list of PII collected.

3. Does this website use web measurement and customization technologies? ☒ Yes ☐ No

FERC uses web measurement and customization technologies to collect information about users' visits to the site. For a more detailed explanation please read "Information collected for website improvement and customization (cookies)".

4. Does this information system use a third-party social media website to communicate and interact with the public? ☐ Yes ☒ No

XXI. CONFIDENTIALITY IMPACT LEVEL

1. Indicate the potential impact that could result to the individual and/or the Commission if PII were inappropriately accessed, used, or disclosed from this information system.

   ☐ Low – The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

   ☒ Moderate – The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

   ☐ High – The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

XXII. PRIVACY IMPACT ASSESSMENT CERTIFICATION

FERC SAOP Signature/Date: Based on the assessment and analysis, I certify that there ☐ are/■ are not any known privacy risks that require mitigation, and security and privacy controls ☐ are/☐ are not appropriately scoped and implemented.	MITTAL DESAI Digitally signed by MITTAL DESAI Date: 2021.04.05 07:51:20 -04'00'
FERC Privacy Officer Signature/Date: Based on the assessment and analysis, I certify that there ☐ are/■ are not any known privacy risks that require mitigation, and security and privacy controls ■ are/☐ are not appropriately scoped and implemented.	ERIC RIPPETOE Digitally signed by ERIC RIPPETOE Date: 2021.03.29 13:26:29 -04'00'
FERC System Owner Signature/Date: I certify that the appropriate confidentiality impact level that pertains to the data has been identified and that baseline or greater security and privacy controls are in place to protect the PII.	KAVEH TAHVILDARY Digitally signed by KAVEH TAHVILDARY Date: 2021.03.25 18:51:08 -04'00'
FERC Information System Security Officer: I certify that the appropriate confidentiality impact level that pertains to the data has been identified and that appropriate privacy and security controls are incorporated at all stages of the life cycle.	KEVIN KELLY Digitally signed by KEVIN KELLY Date: 2021.03.25 18:14:41 -04'00'
Third-Party Chief Privacy Officer: Based on the assessment and analysis, I certify that there ☐ are/☐ are not any known privacy risks that require mitigation, and security and privacy controls ☐ are/☐ are not appropriately scoped and implemented	