# Federal Energy Regulatory Commission

## General Support System (GSS)
## Privacy Impact Assessment (PIA)

March 31, 2020

Federal Energy Regulatory Commission
Cybersecurity & Information Assurance 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** | March 31, 2020 |
| **Author** | Danielle Shorter |
| **Document Title** | General Support System Privacy Impact Assessment (PIA) |

| Owner Details | |
|---|---|
| **Name** | Kaveh Tahvildary |
| **Office/Region** | Federal Energy Regulatory Commission, Washington, DC 20426 |
| **Contact Number** | (202) 502-8430 |
| **E-mail Address** | Kevin.Tahvildary@ferc.gov |

| Revision History | | | |
|---|---|---|---|
| **Version** | **Date** | **Author** | **Comments** |
| 1.0 | January 3, 2017 | Andrew Kosakowski | Initial Document Creation |
| 2.0 | March 10, 2017 | Danielle Nelson | Updated entire document to include all GSS systems and databases |
| 3.0 | March 29, 2017 | Danielle Nelson | Final Release |
| 4.0 | May 3, 2019 | Danielle Shorter | Updated Final Release |
| 5.0 | March 30, 2020 | Danielle Shorter | Updated PIA with new GSS software and storage facility that collects PII. |

## Table of Contents

# 1 INTRODUCTION

## 1.1 PURPOSE AND SCOPE

For all systems subject to the Assessment and Authorization (A&A) process, a Privacy Threshold Assessment (PTA) must be performed. The PTA process consists of the Information System Owner (ISO), or delegate, replying to a survey provided by the Information Security and Systems Assurance Division (ISSAD) team to determine if the system contains any Personally Identifiable Information (PII). When the system contains PII, then a full Privacy Impact Assessment (PIA) must be performed. The PTA satisfies the assessment requirement when the system does not contain PII.

Upon reviewing the survey results for the Federal Energy Regulatory Commission (FERC) General Support System (GSS), it has been determined that the system **DOES** contain PII and a PIA is required.

A questionnaire from the SurveyMonkey tool is the basis for addressing the PII requirement for FERC. The questionnaire results are attached in Appendix A.

# 2 SIGNATURES

## 2.1 PRIVACY OFFICER

I confirm that:

- The above observations are accurate according to the data that has been collected and reviewed
- A reasonable amount of due diligence was taken to make our conclusions

Signature: ERIC RIPPETOE Digitally signed by ERIC RIPPETOE
Date: 2020.04.07 09:28:46 -04'00'

Eric Rippetoe Date

Senior Agency Official for Privacy (SAOP)

## 2.2 SYSTEM OWNER

I confirm that:

- I am in agreement with the above categorizations
- I am aware that the system contains the data as described above.

Signature: KAVEH TAHVILDARY Digitally signed by KAVEH TAHVILDARY
Date: 2020.04.06 09:13:49 -04'00'

Kaveh Tahvildary Date

Information System Owner

## APPENDIX A. PIA QUESTIONNAIRE RESULTS

### SECTION I: PURPOSE OF THE SYSTEM

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.

### SECTION II: DATA IN THE SYSTEM

1. Generally, describe the information to be used in the system in each of the following categories: Public Individual, Employee, Contractor, Other.

   (a) Public Individual: See below

   (b) Employee and Contractor: See below

   (c) Other: See below

   The GSS provides for the internal and external transmission and storage of Commission data. The Commission's system interconnections and various business systems that utilizes the GSS infrastructure and a description of the data used for each of the above 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 their name and e-mail address.

  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 (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 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/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 the 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 Endace; 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.

2. What are the sources of the information in the system?

   The information in the GSS is sourced from the above system interconnections, business dependent systems, and software/storage facility identified in question one. The systems referenced above obtain data from various sources, such as utility companies, private citizens, federal and state agencies, and FERC employees and contractors.

   The sources of the information in the FOIA/CEII Tracker 2.0 is received directly from a private or public requestor through the electronic FOIA/Privacy/CEII request form, or information is manually inserted in the tracker when a request is received by e-mail, mail, or fax. The FOIA liaison may manually enter FOIA/Privacy/CEII requests. In addition, the FOIA/CEII Tracker 2.0 captures the name of the FOIA liaison (the creator of the record), names of the attorney and paralegal assigned to the request, along with the point of contact in each program office.

   Program office employees upload documents to SharePoint based on their level of access permissions or rights as a content manager. The sources of the information contained in the documents uploaded to SharePoint can range from information collected from employees, business entities, or members of the public.

3. What FERC files and databases are used?

FERC uses Network Storage to share, store, and secure FERC information. These network drives are available to all FERC users and access is restricted using Active Directory and Least Access / Least Privilege rights assignment. There are no outside users.

All FOIA/Privacy/CEII requests and responses are captured in the FOIA/CEII Tracker 2.0. Details about requests received by mail, electronic form, e-mail, or fax are included.

There are no databases used.

4. What Federal agencies are providing data for use in the system?

The following Federal agencies provide data that is contained in one or more of the systems identified in question one:

- U.S. Commodity Futures Trading Commission (CFTC)
- Department of Energy (DOE) (U. S. Energy Information Administration (EIA))

No Federal agencies are providing data for use in the FOIA/Privacy/CEII tracker.

No Federal agencies are providing data for use in the Commission’s SharePoint sites.

5. What State and Local Agencies are providing data for use in the system?

State public utility commissions submit tariff filings and rate change applications.

No state or local agencies provide data for use in the FOIA/CEII Tracker 2.0.

No state or local agencies are providing data for use in the Commission’s SharePoint sites.

6. What other third-party sources will data be collected from?

FERC receives information from North American Electric Reliability Corporation (NERC) about reliability trends or reliability gaps that might require development of new or modified reliability standards.

eLibrary contains daily filings and issuances received by FERC from companies, individuals, organizations, government entities, or private citizens. Information is captured in eLibrary and given a record and classification.

A FOIA/Privacy/CEII request also collects information from a third-party representative submitting what’s labeled as non-public material(s) to FERC. After the request is received by FERC, a determination is made whether to release the "non-public information."

Forms and documents in the SharePoint repository contain information obtained from employees, business entities, and members of the public.

7. What information will be collected from the employee, contractor, and/or public individual?

- **FOIA/Privacy/CEII** private and public requestors provide their contact information, such as first and last name or organization name, U.S. home mailing address, e-mail address, business address and telephone number, or international address. In addition, the names of the GAL attorney and paralegal assigned to the request are included along with the program office name and program office staff member responsible for fulfilling the request will be collected in FOIA/CEII Tracker 2.0.

- **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, performance results). The 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."

- **FERC Online** encompasses eComment, eRegister, eFiling, eSubscription, eService, eTariff, and eLibrary, which collects the following types of information:
    - The eComment electronic form can be completed by any individual. This form collects name, address (street, city, state, and zip code), and e-mail

address. This form is completed by individuals submitting comments related to hydroelectric license/re-license proceedings, pre-filing activity for planned natural gas projects, and applications for authorization to construct a natural gas pipeline.

  - The eRegistration, eFiling and eSubscription electronic forms collect first and last name (middle initial is optional) and e-mail address of the public registrant.

  - eTariff and eLibrary are used to run full text searches to see the status of tariff provisions and eLibrary issuances/filings by the Commission.

- FERC employees are required to complete several types of forms that are part of the onboarding process and to maintain employment at the Commission. Various forms are required to be completed from an employees' government furnished computer. There is the potential that an employee may save their completed form(s) to the GSS network. Forms required to be completed during the onboarding process and continued employment with FERC may request the employee to provide information that includes, but is not limited to, their name, date of birth, home address, and SSN (e.g., on their financial disclosure forms).

8. How will data collected from sources other than FERC records and the identified individual be verified for accuracy?

   FERC collects information directly from private citizens, utility companies, 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.

   The information collected from business entities, private citizens, and employees by forms and other types of documents, and uploaded to SharePoint, are relied on to be accurate at the time of collection.

9. How will data be checked for completeness?

   For most of the FERC Online forms, there are required fields that must be completed before submitting a form.

   In addition, there are validation runs/processes for FERC filings to ensure what is being reported is accurate and complete.

   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 and complete. However, the requestor can be contacted to verify contact information.

The information collected from business entities, private citizens, and employees by forms and other types of documents, and uploaded to SharePoint, are relied on at the time of collection to be complete.

10. Is the data current? (yes or no)

    Yes.

11. If the data is current, how do you know?

    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.

    The information collected from business entities, private citizens, and employees by forms and other types of documents, and uploaded to SharePoint, are relied on at the time of collection to be current. If information needs to be updated, it is incumbent upon the individual whom the information is collected from to notify the Commission.

12. Are the data elements described in detail and documented?

    Not applicable.

13. If the data elements are documented in detail, what is the name of the document?
    Not applicable.

## SECTION III: ACCESS TO THE DATA

1. Who will have access to the data in the system? (Select: users, managers, system administrators, developers, other [specify]

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

2. Comments: Access varies per interconnecting and dependent system/application provided in *Section I. Data in the System*, question one. 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

3. How is access to the data by a user determined?

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.

4. Are criteria, procedures, controls, and responsibilities regarding access documented?

   Yes.

5. Comments: SOPs 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.

6. Will the users' access to all data on the system be restricted?

   Yes.

7. Please Explain:

   Users' access depends on the program office per system/application. There are documents in eLibrary that are publicly accessible with no limited access. However, there are certain systems/applications within the Office of Enforcement and the Office of Energy Infrastructure Security (OEIS), as well as other offices, where access is restricted.

In addition, the Activity Tracking Management System (ATMS) is accessible only to Federal staff. This system/application is a workload tracking system that all offices use to track assigned tasks and activities.

SharePoint site users' access to data will be restricted by a program office content manager.

The users of the FOIA/ CEII Tracker 2.0 are restricted about what they can do with the data in terms of changes and modifications. All users have view access to the data.

8. What controls are in place to prevent the misuse (for example, browsing) of data by those having access?

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

   Prior to being granted access to FERC information technology (IT) and data, employees are required to read the "Rules of Behavior for Users of Information Technology" or "Rules of Behavior for Privileged Users" and sign the "Acknowledgement of Rules of Behavior for IT Users." Users acknowledge they are personally responsible for their actions, understand their role as a network user, and will comply with FERC's Rules of Behavior (ROB) for *IT Users Policy*.

   The ROB's responsibilities section addresses protecting information by ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of the data.

   In addition, this section covers providing access to sensitive information after ensuring the parties have the proper authorization and need-to-know. The ROB informs the user of penalties that can be imposed due to non-compliance.

   There are also SOPs that address acceptable use and proper document handling.

   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.

9. Do other systems share data or have access to data in this system?

   Yes.

   FOIA/CEII Tracker 2.0: No.

10. If yes, please explain.

This PIA addresses FERC's GSS, which provides a central source of business system infrastructure for other system interconnections. See *Section I. Data in the System*, question one, for a comprehensive list of GSS interconnections/dependent systems and a list of data shared.

Although, the FOIA/ CEII Tracker 2.0 does not receive data from another system or provide another system with access to the data in the tracker.

11. Who will be responsible for protecting the privacy rights of the following individuals affected by the interface: Employees, Contractors, and Public Individuals?

    All FERC employees and contractors are responsible for protecting the privacy rights of other employees, contractors, and the public.

12. Will any other agencies share data or have access to data in this system? (yes or no)

    Yes.

    Although, no agencies can share data or have direct access to the data in the FOIA/ /CEII Tracker 2.0.

13. Specify any other agencies (International, Federal, State, Local, or Other) that share or have access to the system's data:

    CFTC, DOE (EIA), 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, U.S. Dept. of Treasury, and Department of Interior.

14. How will the data be used by the agency?

    The data in the system will be used to support FERC's mission to "assist consumers in obtaining reliable, efficient and sustainable energy services at a reasonable cost through appropriate regulatory and market means and to perform necessary day-to-day Commission functions."

    FOIA and GAL staff use the information in the FOIA/CEII Tracker 2.0 to respond to FOIA/Privacy/CEII requests.

    Documents and information within SharePoint are used for various reasons. Policies, procedures, and guides are used to educate the Commission workforce on a host of different subject matters. Forms such as the country clearance travel form and other internal and external forms are used to carry out the functions of the Commission.

15. Who is responsible for assuring proper use of the data?

    Proper use and handling of data is governed by the program office and is based on policies and SOPs in place.

16. How will the system ensure that agencies only get the information to which they are entitled?

    To gain access to the FERC Online application, individuals and companies must first register online. Users, for example, may subscribe to specific dockets and may have immediate access to the correspondence or documents in eLibrary. However, before FERC releases data that is not generally available to the public, documents must go through a vetting process prior to release.

    In addition, FERC Online has various electronic forms that are completed by individuals or companies. Information requested by electronic form is a structured set of "questions" to ensure that the information requested and provided is approved for consumption and release by the Commission.

    The information that FERC shares with other Federal, state, local agencies, etc., is that which is in compliance with the Commission's statutes, rules, orders, and policy.

    Information collected in the FOIA/CEII Tracker 2.0 is not shared with other agencies.

## SECTION IV: ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? (yes or no)

   Yes.

2. Explain the relevance and necessity of the use of the data to the purpose(s) of the system:

   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.

   The PII collected in a FOIA/Privacy/CEII request is necessary to respond to a requestor.

3. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? (yes or no)

   No.

4. Comments: The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

5. Will the new data be placed in the individual's records? (yes or no)

   No.

6. Comments: Not applicable.

7. Can/will the system make determinations about identified individuals (members of the public, employees, etc.) that would not be possible without the new data? (yes or no)

   No.

8. Comments: Not applicable.

9. How will the new data be verified for relevance and accuracy?

   Not applicable.

10. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

    Data is being consolidated, for example, in eLibrary. 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 Section I of 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.

11. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

    Yes.

12. Please explain.

    There are security access controls and role-based access controls in place to protect the data and prevent unauthorized access.

    FEMS has a provision for auditing and checking who accessed artifacts.

    There are no processes being consolidated in the FOIA/ CEII Tracker 2.0.

    Program offices provide access restrictions to SharePoint site where the information is sensitive and/or only those with a need to know should have access. To gain access to a SharePoint site/folder that has access restrictions, a request must be submitted to the program office content manager/owner of the site providing a reason why access is needed. Upon approval, access is granted.

13. How will the data be retrieved?

    Data is retrieved in eLibrary by running a general search, to include, but is not limited to: date range (e.g., filed or posted date), category (submittal and/or issuance), library (electric, natural gas, oil, hydro, rulemaking, general), and docket number.

    A search and retrieval can be performed in the FOIA/CEII Tracker 2.0 by the date, request number, requestor's name, subject matter, and the individual assigned to the request.

    In addition, data is retrieved in SharePoint by using the search feature to locate documents. A search can be conducted based on the name of the person who authored a document.

14. Can the data be retrieved by personal identifier?

    GSS: No.

If yes, please explain:

    FOIA/CEII Tracker 2.0: Yes. Data can be retrieved by the requestor's first and last name and the request number assigned to the requestor.

    Documents in SharePoint can be retrieved by the name of the person who authored a document. SharePoint is not a system of records in accordance with the Privacy Act of 1974.

15. What are the potential effects on the due process rights of employees, contractors, and public individuals of the consolidation and linkage of files and systems; derivation of data; accelerated information processing and decision making; use of new technologies?

    There are no potential effects on the due process rights of employees, contractors, and public individuals.

16. How are these potential effects to be diminished? Not applicable.

## SECTION V: MAINTENANCE OF ADMINISTRATIVE CONTROLS

1. Explain how the system and its use will ensure equitable treatment of employees, contractors and public individuals.

   The system or use of the system is not capable of unequal treatment of employees, contractors, and public individuals.

   There are Commission policies and SOPs in place about how to handle data collected, used, disseminated, and shared at FERC.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

   The GSS and all subsystems and applications reside and is operated at FERC Headquarters in Washington, D.C. There are copies of the GSS maintained, but not operated on secondary sites, at the Alternate Computing Facility and the FERC regional offices.

3. Explain any possibility of unequal treatment of individuals or groups.

   There are no possibilities of unequal treatment of individuals or groups because there are no disparate outcomes based on information the system collects.

4. What are the retention periods of data in this system?

   **GSS:** Due to the length of the GSS records retention schedules, the following link has been provided to FERC employees, contractors, and others accessing the schedules internally.

   Select the program office in the link below for a list of records and dispositions.

   http://fercnet/newfercnet/OED/issad/info-gov/inventory.asp

   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.

   http://www.ferc.gov/resources/pub-ref-rm.asp

   **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.

**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.

**Disposition Authority:** DAA-GRS2016-00020002

5. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

   The National Archives Records Administration Records Schedule and the FERC Comprehensive Records Disposition Schedule provides mandatory disposition instructions regarding how to maintain the agency's operational records and what to do with them when they are no longer needed for current business.

   The disposition instructions state whether individual series of records are "permanent" or "temporary," as well as how long to retain the records. Records with historical value, identified as "permanent," are transferred to the National Archives of the United States. All other records are identified as "temporary" and are eventually destroyed in accordance with the Records Schedule.

   FOIA/CEII Tracker 2.0: 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. In accordance with guidance from the Department of Justice, records regarding FOIA requests must be maintained for a minimum of two years if a determination for full release was rendered. Requests that were denied in part or in their entirety must be maintained for a minimum of six years.

6. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

   The eFiling system electronically 'date stamps' each incoming filing. and staff manually checks and approves according to SOPs. Similarly, staff manually date stamps each incoming hard copy filing before indexing and scanning into eLibrary. There are many checks in place governed by their SOPs.

   FOIA/CEII Tracker 2.0: If a FOIA/Privacy/CEII requestor challenges the data in the system, new information provided may be added to the original data, but it is not deleted.

7. Is the system using technologies in ways that the FERC has not previously employed (e.g. Caller-ID)? (yes or no)

Yes.

8. Comments: FERC program offices, such as Office of Electric Reliability and OEIS, are using new technologies not previously used to analyze market trends and to connect different data points.

9. How does the use of this technology affect the privacy of the employee, contractor and public individual?

   New technologies deployed at the Commission to check market trends and analyze data points do not involve PII nor can they affect an individual's privacy.

10. Will this system provide the capability to identify, locate, and monitor individuals? (yes or no)

    Yes.

11. Please explain:

    The system can provide the capability to identify individuals through Active Directory.

    SharePoint can track who has uploaded, modified, or deleted documents.

    ATMS is a workload tracking system that program offices use to track employees' assigned tasks and activities.

12. Will this system provide the capability to identify, locate, and monitor groups of people?

    No.

13. If yes, please explain:

    Not applicable.

14. What controls will be used to prevent unauthorized monitoring?

    Access controls and role-based access controls as described in the System Security Plan will be used to prevent unauthorized monitoring.

    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 changes.

15. Under which System of Records Notice (SORN) does the system operate? Please provide both the number and the name.

    Not applicable. This GSS is not a system or records where information is retrieved by a personal identifier.

    FOIA/CEII Tracker 2.0 SORNs can be accessed at the following links:

    https://www.govinfo.gov/content/pkg/FR-2016-09-07/pdf/2016-21418.pdf

    https://www.govinfo.gov/content/pkg/FR-2014-03-28/pdf/2014-06993.pdf

   SharePoint is not a System of Record as defined in the Privacy Act of 1974.

16. If the system is being modified, will the SORN require amendment or revision?

    Not applicable.

17. Please explain:

    The system is not being modified.

18. What opportunities have individuals been given to decline to provide information (where providing information is voluntary)?

    Not applicable. All information requested is statutorily required. For example, information required in rate filings, as mandated by statute, must be submitted.

    FOIA/Privacy/CEII tracking system: To respond to a FOIA/Privacy/CEII request, 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.

19. What opportunities have individuals been given to consent to uses of the information (other than required or authorized uses), and how do such individuals grant that consent?

    Information collected is only used for required or authorized purposes.