

# Accenture Federal Cloud ERP

## Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA)



Prepared for

**Federal Energy Regulatory Commission**

888 1<sup>st</sup> Street NE

Washington, DC 20426

Prepared by

**Accenture Federal Services**

April 2018

Controlled Unclassified Information

FedRAMP Privacy Threshold Analysis and Privacy Impact Assessment Template



# FedRAMP

Accenture Federal Services LLC


Accenture Federal Cloud ERP

Version 1.3


April 30, 2018

Controlled Unclassified Information

Prepared by

Organization Name that prepared this document		
	Organization Name	Accenture Federal Services LLC
	Street Address	800 N. Glebe Road
	Suite/Room/Building	Suite 300
	City, State, ZIP	Arlington, VA 22203

Prepared for

Organization Name for whom this document was prepared		
	Organization Name	Accenture Federal Services LLC
	Street Address	800 N. Glebe Road
	Suite/Room/Building	Suite 300
	City, State, ZIP	Arlington, VA 22203

Record of Changes for Template

Date	Description	Version	Author
10/31/2016	Initial Publication	1.0	AFS

### Revision History

Complete 15.4 Attachment 4 – PTA and PIA Revision History in the System Security Plan. Detail specific changes in the table below

Date	Version	Page(s)	Description	Author
10/31/2016	1.0		Initial Publication	AFS
12/20/2016	1.1		Updated based on comments from FERC's review	AFS
11/14/2017	1.2	5	Updated response in section 2.1, question 4 to be "Yes" since a SORN does exist. Also, updated reference to SORN ID.	AFS
2/5/2018	1.3	2,5,6,7,8,9 10,11,12,13, 16	Updated based on comments from FERC's review	AFS

#### How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact [info@fedramp.gov](mailto:info@fedramp.gov)

For more information about the FedRAMP project, see [www.fedramp.gov](http://www.fedramp.gov)

Table of Contents

---

1	PRIVACY OVERVIEW AND POINT OF CONTACT (POC).....	1
1.1	Applicable Laws and Regulations.....	1
1.2	Applicable Standards and Guidance .....	3
1.3	Personally Identifiable Information (PII).....	5
2	PRIVACY THRESHOLD ANALYSIS .....	5
2.1	Qualifying Questions .....	5
2.2	Designation .....	6
3	PRIVACY IMPACT ASSESSMENT .....	6
3.1	PII Mapping of Components.....	6
3.2	PII in Use .....	7
3.3	Sources of PII and Purpose .....	8
3.4	Access to PII and Sharing .....	8
3.5	PII Safeguards and Liabilities .....	9
3.6	Contracts, Agreements, and Ownership.....	11
3.7	Attributes and Accuracy of the PII.....	12
3.8	Maintenance and Administrative Controls.....	12
3.9	Business Processes and Technology .....	13
3.10	Privacy Policy .....	14
3.11	Assessor And Signatures.....	14
4	ACRONYMS.....	1

List of Tables

---

Table 1-1	- System Name Privacy POC.....	1
Table 1-2	FedRAMP Laws and Regulations .....	1
Table 1-3	FedRAMP Standards and Guidance .....	3
Table 3-1	PII Mapped to Components.....	6

## 1 PRIVACY OVERVIEW AND POINT OF CONTACT (POC)

The Table 1-1 - System Name Privacy POC individual is identified as the System Name Privacy Officer and POC for privacy at CSP Name.

*Table 1-1 - System Name Privacy POC*

<b>Name</b>	Faisal Mian
<b>Title</b>	AFCE Privacy Officer
<b>CSP / Organization</b>	Accenture Federal Services (AFS)
<b>Address</b>	800 N Glebe Rd, Suite 300, Arlington, VA
<b>Phone Number</b>	571-414-2417
<b>Email Address</b>	Faisal.i.mian@accenturefederal.com

### 1.1 APPLICABLE LAWS AND REGULATIONS

The FedRAMP Laws and Regulations may be found on: [www.fedramp.gov](http://www.fedramp.gov) Templates. A summary of FedRAMP Laws and Regulations are included in the System Security Plan (SSP).

Table 1-2 FedRAMP Laws and Regulations include additional laws and regulations specific to PeopleSoft. These will include laws and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

*Table 1-2 FedRAMP Laws and Regulations*

<b>Identification Number</b>	<b>Title</b>	<b>Date</b>	<b>Link</b>
44 USC 31	Title 44 Public Printing and Documents; Chapter 31 Records Management by Federal Agencies	January 2012	<a href="#">44 USC 31</a>
5 USC 552a	Title 5 Government Organization and Employees; Chapter 5 Administrative Procedure; Section 552a Records maintained on individuals (Privacy Act of 1974 as amended)	January 2014	<a href="#">5 USC 552A</a>
HSPD-12	Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors [HSPD-12], August 27, 2004	August 2004	<a href="#">HSPD-12</a>
HSPD-7	Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and	December 2003	<a href="#">HSPD-7</a>

Identification Number	Title	Date	Link
	Protection [HSPD-7], December 17, 2003		
OMB Circular A-108	Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [, as amended]	Rescinded by OMB A-130	Archived
OMB Circular A-123	Management's Responsibility for Internal Control Revised	December 2004	<a href="#">OMB A-123</a>
OMB Circular A-130	Management of Federal Information Resources, Revised, Transmittal Memorandum No. 4	November 2000	<a href="#">OMB A-130</a>
OMB Circular A-130 iii	Security of Federal Automated Information Systems, Appendix III	November 2000	<a href="#">OMB A-130 Appendix iii</a>
OMB M-01-05	Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy	December 2000	<a href="#">OMB M 01-05</a>
OMB M-03-22	OMB Guidance for Implementing the Privacy Provisions	September 2003	<a href="#">OMB M-03-22</a>
OMB M-04-04	E-Authentication Guidance for Federal Agencies	December 2003	<a href="#">OMB M 04-04</a>
OMB M-06-16	Protection of Sensitive Agency Information	June 2006	<a href="#">OMB M-06-16</a>
OMB M-17-12	Preparing for and Responding to a Breach of Personally Identifiable Information	January 2017	<a href="#">OMB M-17-12</a>
OMB M-10-23	Guidance for Agency Use of Third-Party Websites	June 2010	<a href="#">OMB M-10-23</a>
OMB M-99-18	Privacy Policies on Federal Web Sites	June 1999	<a href="#">OMB M-99-18</a>
PL 99-474	Computer Fraud and Abuse Act , 18 USC 1030	October 1986	<a href="#">PL 99-474</a>
PL 100-503	Consolidated Appropriations Act of 2005, Section 522	October 1988	<a href="#">PL 100-503</a>
PL 104-191	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	August 1996	<a href="#">PL 104-191</a>
PL 104-231	Electronic Freedom of Information Act As Amended in 2002 [PL 104-231, 5 USC 552], October 2, 1996	October 1996	<a href="#">PL 104-231</a>
PL 107-56	USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)	October 2001	<a href="#">PL 107-56</a>
PL 107-347	E-Government Act [includes FISMA Title III]	December 2002	<a href="#">PL 107-347</a>
PL 108-447	Consolidated Appropriations Act of 2005, Section 522	September 2005	<a href="#">PL 108-447</a>
PL 113-187	44 U.S.C The Presidential and Federal Records Act Amendments of 2014 showing changes to NARA	December 2014	<a href="#">PL 113-187</a>

Identification Number	Title	Date	Link
	Statutes found below in Chapters 21, 22, 29, 31, 33, of Title 44 in PDF.		
NARA	44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33 (see Public Law 113-187)	February 2008	<a href="#">NARA 44USC</a>
FTC	Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices	June 2008	<a href="#">FTC Sec-5</a>
NCSL	State Privacy Laws	January 2016	<a href="#">NCSL</a>
ECFR	Title 35, Code of Federal Regulations, Chapter XII, Subchapter B	March 2016	<a href="#">e-CFR data</a>

## 1.2 APPLICABLE STANDARDS AND GUIDANCE

The FedRAMP Standards and Guidance may be found on: [www.fedramp.gov](http://www.fedramp.gov) Templates. The FedRAMP Standards and Guidance are included in the System Security Plan (SSP ATTACHMENT 12 – FedRAMP Laws and Regulations. For more information, see the Program Documents Overview section of the FedRAMP website.

Table 1-3 FedRAMP Standards and Guidance includes any additional standards and guidance specific to PeopleSoft. These will include standards and guidance from Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP).

*Table 1-3 FedRAMP Standards and Guidance*

Identification Number	Title	Date	Link
FIPS PUB 140-2	Security Requirements for Cryptographic Modules	May 2001	<a href="#">FIPS 140-2</a>
FIPS PUB 199	Standards for Security Categorization of Federal Information and Information Systems	February 2004	<a href="#">FIPS 199</a>
FIPS PUB 200	Minimum Security Requirements for Federal Information and Information Systems	March 2006	<a href="#">FIPS 200</a>
FIPS PUB 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors	August 2013	<a href="#">FIPS 201-2</a>
NIST SP 800-18	Guide for Developing Security Plans for Federal Information Systems, Revision 1	February 2006	<a href="#">SP 800-18</a>
NIST 800-26	Security Self-Assessment Guide for Information Technology Systems	Superseded By: FIPS 200, SP 800-53, SP 800-53A	<a href="#">Archived NIST SP</a>
NIST SP 800-27	Engineering Principles for Information Technology Security Revision A (A Baseline for Achieving Security)	June 2004	<a href="#">SP 800-27</a>



Identification Number	Title	Date	Link
NIST SP 800-30	Guide for Conducting Risk Assessments, Revision 1	January 2015	<a href="#">SP 800-30</a>
NIST SP 800-34	Contingency Planning Guide for Federal Information Systems Revision 1 [includes updates as of 11-11-10]	May 2010	<a href="#">SP 800-34</a>
NIST SP 800-37	Guide for Mapping Types of Information and Information Systems to Security Categories (Revision 1)	February 2010	<a href="#">SP 800-37</a>
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View	March 2011	<a href="#">SP 800-39</a>
NIST 800-47	NIST 800-47, Security Guide for Interconnecting Information Technology Systems	August 2002	<a href="#">SP 800-47</a>
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4 [Includes updates as of 01-22-2015]	April 2013	<a href="#">SP 800-53</a>
NIST SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Revision 4	December 2014	<a href="#">SP 800-53A</a>
NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories, Revision 1	August 2008	<a href="#">SP 800-60</a>
NIST SP 800-61	Computer Security Incident Handling Guide, Revision 2	August 2012	<a href="#">SP 800-61</a>
NIST SP 800-63-2	Electronic Authentication Guideline: Computer Security, Revision 2	August 2013	<a href="#">SP 800-63-2</a>
NIST SP 800-64	Security Considerations in the System Development Life Cycle, Revision 2	October 2008	<a href="#">SP 800-64</a>
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment	September 2008	<a href="#">SP 800-115</a>
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems	August 2011	<a href="#">SP 800-128</a>
NIST SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations	September 2011	<a href="#">SP 800-137</a>
NIST SP 800-144	Guidelines on Security and Privacy in Public Cloud Computing	December 2011	<a href="#">SP 800-144</a>
NIST SP 800-145	The NIST Definition of Cloud Computing	September 2011	<a href="#">SP 800-145</a>
FTC	Privacy Online: Fair Information Practices in the Electronic	June 1998	<a href="#">FTC Privacy Online</a>

Identification Number	Title	Date	Link
	Marketplace: A Federal Trade Commission Report to Congress		
NARA 2010-05	Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin)	September 2010	<a href="#">NARA 2010-05</a>
FDIC	Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks	June 2004	<a href="#">FDIC Privacy Risks</a>

### 1.3 PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) as defined in OMB Circular A-130 refers to 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. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

- Social Security numbers
- Passport numbers
- Driver’s license numbers
- Biometric information
- DNA information
- Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

## 2 PRIVACY THRESHOLD ANALYSIS

Accenture Federal Services (AFS) performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the Accenture Federal Cloud ERP (AFCE) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by AFS can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

### 2.1 QUALIFYING QUESTIONS

- Yes            1. Does the Interconnection Security Agreement (ISA) collect, maintain, or share PII in any identifiable form?
- Yes            2. Does the ISA collect, maintain, or share PII information from or about the public?
- Yes            3. Has a Privacy Impact Assessment ever been performed for the ISA?
- Yes            4. Is there a Privacy Act System of Records Notice (SORN) for this ISA system?  
If yes; the SORN identifier and name is: Federal Energy Regulatory Commission (FERC) Management, Administrative, and Payroll System (MAPS) Financials (FERC-36). This SORN is in the process of being modified and will republished in the Federal Register as PeopleSoft.

If answers to Questions 1-4 are all “No” then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment.

## 2.2 DESIGNATION

Check one.

- A Privacy Sensitive System
- Not a Privacy Sensitive System (in its current version)

## 3 PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment has been conducted for the AFCE on 3/6/2018.

### 3.1 PII MAPPING OF COMPONENTS

AFCE consists of 3 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by AFCE and the functions that collect it are recorded in Table 3-1 PII Mapped to Components.

*Table 3-1 PII Mapped to Components*

Components	Does this function collect or store Personally Identifiable Information (PII)? (Yes/No)	Type of Personally Identifiable Information (PII)	Reason for Collection of Personally Identifiable Information (PII)	Safeguards
PeopleSoft Financials	Yes	Bank account number, corporate credit card number, name, home address and Taxpayer Identification Numbers such as a Social Security Number (SSN) and Employer’s Identification Number (EIN)	Vendor disbursements, travel reimbursements, tax reporting, and tuition reimbursement	Role-based Access (RBAC) is used to restrict access to PII based on job function and role. A123 Process is an audit logging and reporting process that tracks role changes, logon events, and user access. Data-at-rest encryption is applied as a safeguard to all interface files containing PII data. Interface files are encrypted after processing
Microsoft BI Solution	No	N/A	N/A	N/A

Components	Does this function collect or store Personally Identifiable Information (PII)? (Yes/No)	Type of Personally Identifiable Information (PII)	Reason for Collection of Personally Identifiable Information (PII)	Safeguards
PeopleSoft Human Resources (HR) (Database archive only)	Yes	Employee: Name, home address, date of birth (DOB), payroll data, payroll benefits and deduction enrollment. Dependents/Beneficiaries: Name, home address, DOB	Historical data reporting and analytical purposes	Safeguards applied are Database Password Controls and Read-only data access. RBAC access is restricted to HR personnel based on job function; currently restricted to one user

### 3.2 PII IN USE

Complete the following questions:

1. What PII (name, social security number, date of birth, address, etc.) is contained in the Accenture Federal Services LLC service offering?
  - a. Personal Financial data: An individual’s name, home address, SSN, and corporate credit card are collected only when required to complete a financial reimbursement to the individual, e.g., employee travel expense reimbursement or tuition reimbursement. An individual’s bank account type (e.g., checking or savings), bank routing number, and bank account number are collected to accomplish direct deposits of financial reimbursements.
  - b. Business Financial data: SSN and EIN are collected to identify for payment and tax reporting purposes for the Internal Revenue Services.
  - c. Employee HR data: Employee name, home address, DOB, payroll data, payroll benefits and deduction enrollment and, dependents’ and beneficiaries’ name, home address, and DOB are stored for archival and inquiry purposes.
2. Can individuals “opt-out” by declining to provide PII or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

This question does not apply directly to AFCE because the system does not collect PII directly from individuals. FERC, however, collects information directly from the individual. Individuals may decline to provide information.

- Yes Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):  
At the time FERC collects PII, individuals may decline to provide the requested information, however, this will impact the agency’s ability to issue financial

disbursements to the individual or business. Individuals share information for the purpose of receiving financial reimbursement.

No [Click here to enter explanation.](#)

### 3.3 SOURCES OF PII AND PURPOSE

3. Does Accenture Federal Services LLC have knowledge of federal agencies that provide PII to the system?

Yes. AFS staff have knowledge of federal agencies that provide PII to the system since AFS is responsible for providing the support and maintenance of the application.

4. Has any agency that is providing PII to the system provided a stated purpose for populating the system with PII?

Yes.

5. Does Accenture Federal Services LLC populate the system with PII? If yes, what is the purpose?  
No.

6. What other third party sources will be providing PII to the system? Explain the PII that will be provided and the purpose for it.

a. E-Gov Travel Service (ETS2): Concur/ETS2 is a government-wide travel management system owned by the Government Services Administration (GSA) and is used by federal employees to manage travel authorizations, vouchers and expenditures. PII provided: name, home address, SSN, and corporate credit card.

b. Department of the Interior, Interior Business Center (DOI/IBC), Federal Personnel Payroll System (FPPS). DOI/IBC FPPS transmits a payroll file which contains cost and personal information. PII provided: name, SSN, and Employee ID to financial system for processing the payroll journal accounting entries.

c. Automatic Acquisition Management Solution (AAMS): Transmits vendor information to establish/match vendor profiles in the financial system needed for financial disbursements and tax reporting purposes. Information provided: vendor name, business address, and EIN.

### 3.4 ACCESS TO PII AND SHARING

7. What federal agencies have access to the PII, even if they are not the original provider? Who establishes the criteria for what PII can be shared?

PII is shared with United States Treasury Secure Payment System (SPS) for vendor disbursements and employee reimbursements.

Additionally, PII is shared with Internal Revenue Service (IRS) for tax reporting purposes.

FERC establishes the criteria for what PII can be shared.

8. What AFS personnel will have access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for AFS personnel to have access to the PII.

AFS personnel with access to PII collected by FERC is limited to authorized individuals supporting the AFCE PeopleSoft system and require access to PII to perform their official duties.

This includes:

- System support personnel – to provide production support to system users
- System developers – to perform system design and development
- System administrators – to perform system maintenance and administration

9. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval?

Access is determined by role and need to access PII, upon authorization by the AFCE project manager and the FERC system owner, and completion of a background investigation. Access credentials are created based on employee role in support of the purposes described in AFS AFCE System Security Plan, section 9.3. This section lists the types of users and their sensitivity level:

- AFCE personnel – may also have access to perform tasks relative to the cloud platform
- Information Technology (IT) support staff – may gain access using separate accounts that carry with them administrative (elevated) privileges greater than what is held by most internal users. Refer to the AFS AFCE System Security Plan section 9.3 list of user types and sensitivity levels)
- Network authentication credentials – are authorized and granted by the System Security Administrator for all users (regular and elevated) after they have passed a background verification

All users who have been granted access to the system in the process described above are required to acknowledge and sign a “Sensitive PII Rules of Behavior (ROB)” governing the use of their administrative account.

Approval: All access requires management and government approval.

10. Do other systems share, transmit, or have access to the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing.

The AFCE receives PII transmitted from the AAMS, FERC’s acquisition management system. The PII transmitted from AAMS is used for processing vendor disbursements.

### **3.5 PII SAFEGUARDS AND LIABILITIES**

11. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?

AFS requires all staff and contractors to sign client data protection forms including reading AFS policies. AFS requires all AFCE staff with access to PII, to protect PII. Non-disclosure agreements are established with each subcontractor that prohibits the misuse of client data. All personnel are required to go through a background check prior to being granted access to the application.

A123 process (audit logging and reporting) includes database logging of activities performed by authorized users and is reviewed by the system owner monthly. These logs are used to identify anomalies, data access, and capture authentication information including successful and unsuccessful logon events.

12. Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability?

AFS corporate learning mandates staff to complete annual client data protection training. Standard Operating Procedures (SOPs) and policy around handling PII have been established. Staff are accountable to read and comply with the below policies and practices:

- a. Policy AFS-0053 – External Personnel Access to Company Systems
- b. Policy AFS-0056 – Systems Security
- c. Policy AFS-0057 – Information Security and Acceptable Use of Systems
- d. Policy AFS-0069 – Confidentiality
- e. Policy AFS-0123 – Archives and Records Management.
- f. Complete all corporate required and engagement-specific training related to data privacy, data protection and information security before accessing client data

FERC is responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or stored on the system. The Commission established procedures for handling PII as set forth in *Procedures on Handling FERC-Controlled Personally Identifiable Information*, requiring employees and contractors to complete FERC Security and Privacy Awareness Training, New Hire IT Security and Privacy Training, and Annual IT Security and Privacy Training. Also, employees and contractors are required to sign and acknowledge FERC IT ROB to protect the privacy rights of individuals.

13. Does the AFS annual security training include privacy training? Does AFS require contractors to take the training?

Yes. On an annual basis, apart from corporate training, the AFS AFCE privacy officer conducts privacy focused training for all staff and contractors with access to PII.

14. Who is responsible for assuring safeguards for the PII?

For the AFCE system, AFS and FERC are responsible.

15. What is the magnitude of harm to the corporation if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the corporation be affected?

The magnitude of harm or impact would ultimately depend on the nature of the PII data and the threat exploiting the vulnerability that would have caused the initial breach of confidentiality, availability, or integrity of the data. The reputation of the AFS would be significantly affected, if, an after-the-fact investigation revealed that either the AFS or the customer did not secure the system properly or sufficiently at the infrastructure level (AFS) or application level (AFS/FERC).

16. What is the magnitude of harm to the individuals if privacy related data is disclosed, intentionally or unintentionally?

The magnitude of harm or impact to an individual would ultimately depend on the nature of the PII data and the threat exploiting the vulnerability that would have caused the initial breach of confidentiality, availability, or integrity of the data.

17. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes, subcontractors will provide maintenance of the system. All subcontractors are required to sign an NDA. Additionally, all AFS personnel with access to PII are required to sign a FERC NDA.

18. Is the PII owner advised about what federal agencies or other organizations share or have access to the data?

Yes. Each PII owner is aware of AFCE cloud module structure, which segregates, physically and logically, one federal information system from another.

### **3.6 CONTRACTS, AGREEMENTS, AND OWNERSHIP**

19. NIST SP 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this accountability described in contracts with customers? Why or why not?

Yes. This principle is covered in AFS contracts. As a cloud provider, AFS accepts limited liability in the event AFS fails to deliver its security services as defined in each contract. For example, the following is an extract from one of our standard agreements, "Except for any security services that AFS provides as part of the Services as specifically described in a Service Schedule and for theft, embezzlement, or fraud by AFS or AFS's employees, Client is responsible for the security of Client Data, other Client resources and Client-provided equipment (other than the physical security for any client provided equipment hosted at any AFS facility)."

20. Do contracts with customers establish who has ownership rights over data including PII?

Yes. The AFS contract with FERC states "All documentation, electronic data and information collected or generated by the Contractor in support of this contract shall be considered Government property, and shall be returned to the Government at the end of the performance period."

21. Do contracts with customers require that customers notify AFS if the customer intends to populate the service platform with PII? Why or why not?

AFS requires each customer to disclose if PII will be included in their infrastructure during the pre-sales process. Customer infrastructure requiring PII protection is designed with security protections appropriate to secure PII data. Historically the requirement to notify AFS in the event of a change in PII status has not been included in our contracts. Currently and going forward, however, customer's PII requirements are specified in each customer contract, and the customer is obligated to notify AFS of any changes to customer's PII requirements.

22. Do AFS contracts with customers establish record retention responsibilities for both the customer and AFS?



Yes. AFS retains financial and contracts records for a period of three (3) years, or such other period of time as determined in a specific agreement. With respect to client data, AFS destroys all Client data as appropriate promptly upon the termination of each agreement.

23. Is the degree to which AFS will accept liability for exposure of PII clearly defined in agreements with customers?

Yes. AFS only accepts limited liability for exposure of PII to the extent that AFS breaches the delivery of the security services agreed upon in the contract. The limits to this liability are clearly defined in the *Limitation of Liability* section of our contracts with our Clients.

### **3.7 ATTRIBUTES AND ACCURACY OF THE PII**

24. Is the PII collected verified for accuracy? Why or why not?

FERC has a trusted relationship with DOI/IBS, U.S. Dept. of the Treasury/SPS, and Concur/ETS2 (GSA). As federal agencies, they have a responsibility in assuring that the data provided to FERC is accurate and current. Furthermore, FERC analyzes and reconciles all data transmissions and reconciles transactions monthly.

25. Is the PII current? How is this determined?

When any data is transferred into the system, the system enforces a variety of edits and business rules to assure that all necessary pieces of information are present before it processes the data.

### **3.8 MAINTENANCE AND ADMINISTRATIVE CONTROLS**

26. If the system is operated in more than one site, how is consistent use of the system and PII maintained in all sites? Are the same controls be used?

The Disaster Recovery (DR) site in Colorado has the same configuration and controls as the production site

27. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines?

Data retention guidelines and periods are determined by FERC. The PII data retention is based on what is required to provide the service for which it is collected. Records are destroyed when the Commission determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

FERC applies the retention schedule available in the General Records Schedule 5.2: Transitory and Intermediary Records (GRS 5.2 Item 020 Intermediary Records: <https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf>).

28. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures?

At the end of the retention period, FERC destroys records upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Any reports which contain PII data have a banner to notify the user on the proper disposal methods. AFCE limits the storage of electronic versions of those reports within the AFCE to two (2) weeks.

For decommissioning, AFS employs use of the Department of Defense DoD 5220.22-M 3pass standard to erase all data on any component of the AFCE which contain PII. AFS and FERC jointly establish and agree to the decommissioning procedures employed.

29. Is the system using technologies that contain PII in ways that have not previously deployed? (e.g., smart cards, caller-ID, biometrics, PIV cards, etc.)?

No.

30. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology?

Not applicable.

31. Is access to the PII being monitored, tracked, or recorded?

Access to PII is monitored. AFCE staff and contractors with access to FERC data are required to sign ROB. The rules explicitly detail the permissible and appropriate access and actions required when working with PII.

The system includes A123 audit capabilities which tracks and records access to data, authorized and unauthorized login attempts, and access anomalies. The events are recorded in the A123 report and reviewed and dispositioned to permit the detection and/or prevention of unauthorized access or inappropriate usage of PII.

The A123 report is generated by reading the information within the security and audit tables, the application logs, and database logs. For database access a report is generated by reading the information in Microsoft (MS) Structured Query Language (SQL) server.

The Application Information System Security Officer (ISSO) reviews the A123 reports monthly. Database and Application Administrators review database, application monitoring events, and alerts daily. The FERC Security Administrator tracks application activities monthly for any changes using information such as “modification date” and “modified by.”

32. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision?

Yes

### **3.9 BUSINESS PROCESSES AND TECHNOLOGY**

33. Does the conduct of this PIA result in circumstances that require changes to business processes?

No.

34. Does the completion of this PIA potentially result in technology changes?

No.

### 3.10 PRIVACY POLICY

35. Is there an AFS privacy policy and is it provided to all individuals whose PII you collect, maintain or store?

Yes, there is an AFS privacy policy. AFS corporate learning mandates that all staff and contractors complete required privacy training on an annual basis. All AFS staff and contractors are required to read and comply with the below policies:

- a. Policy AFS-0053 - External Personnel Access to Company Systems
- b. Policy AFS-0056 - Systems Security
- c. Policy AFS-0057 - Information Security and Acceptable Use of Systems
- d. Policy AFS-0069 - Confidentiality
- e. Policy AFS-0123 - Archives and Records Management.

The AFS privacy policy is not provided to individuals whose PII is stored in the AFCE since AFS is not responsible for the collection or maintenance of PII data. Collection and maintenance of PII data is FERC responsibility.

The Simplified Vendor Express Enrollment Form, ALT SF 3881 issued to FERC employees/vendors request the applicant to provide PII to pay/reimburse for travel expenses. A Privacy Act Statement is provided on the form in compliance with the Privacy Act of 1974, and explains that the form is used for collecting data necessary to pay electronically and is required under the provisions of 31 U.S.C. 3332 and 7701. Employees/vendors completing this form are referred to the FERC policy for PII handling guidance when submitting documents containing Controlled Unclassified Information/ Privacy (CUI/PRVCY).

36. Is the privacy policy publicly viewable? If yes, provide the URL:

No.

### 3.11 ASSESSOR AND SIGNATURES

This Privacy Impact Assessment has been conducted by *the AFCE Project Manager for FERC* and has been reviewed by the AFCE, Chief Privacy Officer for accuracy.

---

System Owner Signature

Name **Geoff Gilliar**

Date **3/22/2018**

---

FERC Senior Agency Official for Privacy

Name **Christina Handley**

Date **4/30/2018**



---

Assessor Signature

Name **Ryan Dietrich**

Date **4/30/2018**



---

CSP Chief Privacy Officer Signature

Name **Christopher Copeland**

Date **4/30/2018**

#### 4 ACRONYMS

<b>Acronym</b>	<b>Definition</b>
<b>AAMS</b>	Automatic Acquisition Management System
<b>AFCE</b>	Accenture Federal Cloud ERP
<b>AFS</b>	Accenture Federal Services
<b>BI</b>	Business Intelligence
<b>CSP</b>	Cloud Service Provider
<b>CUI/PRVCY</b>	Controlled Unclassified Information/ Privacy
<b>DOI/IBC</b>	Department of the Interior, Interior Business Center
<b>DOB</b>	Date of Birth
<b>DR</b>	<u>Disaster Recovery</u>
<b>EIN</b>	Employer's Identification Number
<b>FERC</b>	Federal Energy Regulatory Commission
<b>FIPS</b>	Federal Information Processing Standard
<b>FISMA</b>	Federal Information Security Management Act
<b>FPPS</b>	Federal Personnel Payroll System
<b>GSA</b>	Government Services Administration
<b>HR</b>	Human Resource
<b>HRMS</b>	Human Resource Management System
<b>HSPD</b>	Homeland Security Presidential Directives
<b>IRS</b>	Internal Revenue Service
<b>ISA</b>	Interconnection Security Agreement
<b>ISSO</b>	Information System Security Officer
<b>IT</b>	Information Technology
<b>MAPS</b>	Management, Administrative, and Payroll System
<b>NDA</b>	Non-Disclosure Agreement
<b>NIST</b>	National Institute for Standards and Technology
<b>OMB</b>	Office of Management and Budget
<b>POC</b>	Point of Contact
<b>PII</b>	Personally Identifiable Information
<b>PL</b>	Public Law
<b>PTA</b>	Privacy Threshold Analysis
<b>RBAC</b>	Role Based Access
<b>ROB</b>	Rules of Behavior

<b>Acronym</b>	<b>Definition</b>
<b>SORN</b>	System of Records Notice
<b>SP</b>	Special Publications
<b>SPS</b>	Secure Payment System
<b>SSN</b>	Social Security Number
<b>SSP</b>	System Security Plan
<b>TIN</b>	Taxpayer Identification Number
<b>USC</b>	United States Code