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

Prepared by

Federal Energy Regulatory Commission

888 First Street N.E.

Washington, DC 20426

August 11, 2017

FedRAMP Privacy Threshold Analysis

and Privacy Impact Assessment Template

FERC Enterprise Messaging System 2

Enter Version Number 1.0

August 11, 2017

Prepared by

Federal Energy and Regulatory Commission		
	Street Address	888 First Street N.E.
	Suite/Room/Building	N/A
	City, State, ZIP	Washington, D.C. 20426

Prepared for

Federal Energy and Regulatory Commission		
	Street Address	888 First Street N.E.
	Suite/Room/Building	N/A
	City, State, ZIP	Washington, D.C. 20426

Revision History

Date	Version	Page(s)	Description	Author
August 11, 2017	1.0	All	Final Release	Danielle Nelson

Table of Contents

List of Tables

How To Contact Us

For questions about FedRAMP or this document, email to info@fedramp.gov.
For more information about FedRAMP, visit the website at http://www.fedramp.gov.

1. PRIVACY OVERVIEW AND POINT OF CONTACT (POC)

Table 1 – FERC Enterprise Messaging System (FEMS2) Privacy POC

Name	Christina Handley
Title	Senior Agency Official for Privacy
CSP / Organization	Federal Energy and Regulatory Commission
Address	888 First Street N.E., Washington, D.C. 20426
Phone Number	202-502-6500
Email Address	christina.handley@ferc.gov

1.1. PRIVACY LAWS, REGULATIONS, AND GUIDANCE

A summary of laws, and regulations related to privacy include:

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104-231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100-503, Computer Matching and Privacy Act of 1988
- E-Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A-130, Management of Federal Information Resources, 1996
- OMB Memo M-10-23, Guidance for Agency Use of Third-Party Websites
- OMB Memo M-99-18, Privacy Policies on Federal Web Sites
- OMB Memo M-03-22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws

Guidance on privacy issues can be found in the following publications:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
- Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress
- https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission
- Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin)
- http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html
- Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks

https://www.fdic.gov/regulations/examinations/offshore/offshore_outsourcing_06-04-04.pdf

1.2. PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) as defined in OMB Memo M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying 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

The Federal Energy Regulatory Commission (FERC) performs a Privacy Threshold Analysis (PTA) annually to determine if PII is collected by FERC Enterprise Messaging System 2 (FEMS2). If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment (PIA) template used by FERC can be found in Section 3. This section constitutes the PTA and findings.

2.1. QUALIFYING QUESTIONS

FEMS2 is an outsourced information system. FEMS2 uses two outsourced service providers to support and deliver its core services; a bundle of services including email from Microsoft, and Mobile Device Management services from IBM Communications.

1) Does FEMS2 collect, maintain, or share PII in any identifiable form?

Yes

2) Does FEMS2 collect, maintain, or share PII information from or about the public?

Yes

3) Has a Privacy Impact Assessment ever been performed for the FEMS2?

No

4) Is there a Privacy Act System of Records Notice (SORN) for this system?

No

If "Yes," the SORN identifier and name is:

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[1]
☐ Not a Privacy Sensitive System (in its current version)

[1] A Privacy Sensitive System is any system that collects, uses, disseminates, or maintains personally identifiable information (PII) or sensitive PII.

3. PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment is currently being developed for Federal Energy Regulatory Commission Enterprise Messaging System 2 (FEMS2) because this system contains personally identifiable information (PII) on the general public and sensitive PII about FERC employees.

3.1. PII MAPPING OF COMPONENTS

FEMS2 does not consist of any components. Leveraged service provider components are not in the FEMS2 boundary.

Table 2 - PII Mapped to Components

Components	Does this function collect or store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
N/A	N/A	N/A	N/A	N/A

3.2. PII IN USE

Complete the following questions:

1) What PII (name, social security number, date of birth, address, etc.) is contained in FEMS2?

Employees may send e-mails or attachments that include the following information:

- Full name, home address, or personal e-mail address. There is a possibility that an employee may also include their social security number in an e-mail.
- Medical documents that contain employees' full name, and medical diagnosis based on reasonable accommodations, assistive technology and accessibility pursuant to the Americans with Disabilities Act.
- Employee personnel documents (and other new hire/continued employment/retirement personnel documents) that request the employees' full name, social security number, date of birth, and basic pay.

Private citizens and customers may contact FERC through e-mail. An individual may include in their e-mail correspondence their full name, home address, telephone number, and personal e-mail address.

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)?

☒ Yes Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

Employees are not required or encouraged to send PII through e-mail channels. In the event employees' use FERC's internal e-mail system to send PII or sensitive PII, they are required by policy to use proper safeguards such as encryption and password protection.

Private citizens are not required to include PII in their correspondence to FERC. However, in order to research or respond to their inquiry, at minimum, a contact name and e-mail address is necessary to provide a response.

☐ No The employee is not able to opt out of providing the necessary PII to process the employees' request for reasonable accommodation form(s) or employment documentation.

3.3. SOURCES OF PII AND PURPOSE

3) Does FERC have knowledge of federal agencies that provide PII to the system?

There are no federal agencies that provide PII to FEMS2

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

N/A

5) Does the Cloud Service Provider (CSP) 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.

There are no third-party sources providing PII to FEMS2

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?

Federal agencies do not have access to the PII in FEMS2. PII is not shared with federal agencies; therefore, a criteria for what PII can be shared is not necessary.

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

FEMS2 utilizes the following distinct roles:

- **Standard User Role**

  FEMS2 has a single user role for accessing the user level shared resources.

- **FEMS2 Administrator Role**

  The FEMS2 administrator role encompasses administering the Microsoft Office 365 (O365) security group, user provisioning issues, Active Directory Federation Service (ADFS) administration, managing Windows desktops and laptops with Outlook, and addressing issues with single sign-on.

- **O365 Management Console Administrator Role**

  FEMS2 Administrators will access the user provisioning and overall service configuration settings. FEMS2 administrators will use a web browser connecting over the Internet to the Microsoft environment. The O365 administrator console configures the various Microsoft O365 applications, perform user administration, and configure account and application settings. A FERC administrator account can use the console to activate additional services and adjust settings. The default setup includes a set of five hierarchical administrator roles for implementing least privilege and separation of duties.

- **IBM MaaS360 Administrator Role**

  FEMS2 MaaS360 Administrators will access the device provisioning and overall mobile device management (MDM) service configuration settings via the MaaS360 Management Console. FEMS2's administrators can use this console to perform user administration, configure account and application settings, register new devices, set policies, view dashboards, and run reports. FEMS2 administrators may elect to use multifactor authentication for access to the MaaS360 Management Console. In MaaS360's implementation of multifactor authentication, console users log in in with a user name and password and then prior to being allowed access are sent a one-time password via a Short Message Service (SMS) text message or an email for a second login.

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

Microsoft requires that FERC utilize Microsoft Active Directory Federation Services (ADFS) for user provisioning, identity management, authentication, and permissions management. This means that customers must have an existing Active Directory infrastructure. All authentication requests (including requests made with multi-factor credentials) come back to FERC's ADFS endpoint, which authenticates that request, and, upon approval, generates a Security Assertion Mark-up Language (SAML) token; this token contains permissions information, which O365

multi-tenant (MT) honors. Detailed information about ADFS is on TechNet. Use of ADFS is required for FedRAMP-compliant use of O365 MT.

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.

No

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?

Information that is processed, stored, or transitioned to FEMS2 has unauthorized access protections. The information requires safeguards to ensure its confidentiality, integrity, and availability while under Commission control.

Personnel are screened, trained, and monitored. For exact details on how access is granted to customer data, please review the PS, PL, AT, and AU controls in the FEMS2 System Security Plan (SSP). Microsoft recommends focusing on these controls:

- PS-3 Personnel Screening
- PL-4 Rules of Behavior
- AT-3 Security Training
- AU-2 Auditable 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?

All FERC employees and contractors, and CSP, who have access to FEMS2 are responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system.

FERC has established policies and procedures for the proper handling of PII collected, maintained, or shared throughout the Commission.

In addition, the FERC workforce receives Annual Mandated Security and Privacy Awareness Training to understand their responsibility for protecting the PII the Commission collects, maintains or shares.

13) Does the CSP annual security training include privacy training? Does CSP require contractors to take the training?

Microsoft's ongoing training commitments are explained in the AT controls in the SSP.

- AT-2 Security Awareness
- AT-3 Security Training

All FERC employees, contractors, and subcontractors who have access to FERC's data and information systems are required to complete FERC's Annual Mandated Security and Privacy Awareness Training.

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

The FEMS2 system owner is responsible for implementing appropriate security and privacy controls to safeguard the PII in the system.

15) What is the magnitude of harm to the CSP Corporation if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customer be affected?

The security category for the data in FEMS2 has a moderate confidentiality level due to the types of PII.

The risk and magnitude of harm from the loss, misuse, or unauthorized access to or modification of transitioned information in FEMS2 could negatively affect the Commission and CSP's reputation.

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

The disclosure of privacy-related information would have a serious adverse effect to individuals, but does not involve loss of life or serious life threatening injuries.

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?

Any contractors involved in the design or maintenance of Office 365 are subjected to Microsoft's vendor management program as explained in the *System and Services Acquisition Family* of controls in the SSP.

CSP Microsoft maintains the O365 system by applying software updates (i.e., patches) necessary to address system and software vulnerabilities.

Contractors and all personnel assigned to the contract that requires access to FERC's network must sign a Non-Disclosure/Confidentiality Agreement.

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

There are no federal agencies that share or have access to the data.

Microsoft personnel has access to the data in the system.

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 principle described in contracts with customers? Why or why not?

FEMS2 is FERC's enterprise e-mail system and scheduling service that has been outsourced to the Microsoft Cloud. FERC is the information owner and is ultimately accountable for the security and privacy of the data the service provider processes, stores, or transmits. FERC's responsibilities for the information maintained in the cloud is sufficiently addressed in the contract and formal agreement with the cloud service provider.

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

All data is and shall remain the property of FERC.

FERC is the information owner and is ultimately accountable for the security and privacy of the data the service provider processes, stores, or transmits. FERC's responsibilities for the information maintained in the cloud is sufficiently addressed in the contract and formal agreement with the cloud service provider.

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

FERC is not required to notify Microsoft if it intends to populate Office 365 with PII. Microsoft assumes that customers will populate address book/directory data into Office 365 as a standard part of business. Any other use of Office 365 for the transmission, storage, or processing of PII

is subject to agency-specific rules of behavior. Agencies should not populate data above the Federal Information Processing Standard (FIPS) 199 moderate rating into Office 365.

FERC shall retain access and download capability of all data for research, investigation, transfer, or migration to the systems at its discretion.

22) Do CSP contracts with customers establish record retention responsibilities for both the customer and the CSP?

Microsoft's data retention standards are explained in Office 365 Trust Center:
https://products.office.com/en/business/office-365-trust-center-cloud-computing-security

Microsoft contracts reflect data shown in the Trust Center, such as:

> At the end of a customer's subscription or use of the service, the customer may always export its data. Full details are contained within the Product Use Rights (which is the authoritative source on this topic), however, for convenience, the provisions current as of the release of Office 365 are included below:
>
> Online Service Expiration or Termination. Upon expiration or termination of your online service subscription, you must contact Microsoft and tell us whether to:
>
> - (1) disable your account and then delete the customer data; or
> - (2) retain your customer data in a limited function account for at least 90 days after expiration or termination of your subscription (the "retention period") so that you may extract the data.
> - If you indicate (1), you will not be able to extract the customer data from your account. If you indicate (2), you will reimburse us for any applicable costs. If you do not indicate (1) or (2), we will retain the customer data in accordance with (2).
> - Following the expiration of the retention period, we will disable your account and then delete the customer data. Cached or back-up copies will be purged within 30 days of the end of the retention period.
>
> No Liability for Deletion of Customer Data. You agree that, other than as described in these terms, we have no obligation to continue to hold, export or return the customer data. You agree that we have no liability whatsoever for deletion of the customer data pursuant to these terms.

See response to question 27 the data retention schedule established by FERC for e-mails.

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

The Microsoft CSP service level agreement does not appear to accept liability for the exposure of PII.

The Microsoft CSP contractor, Technosource Information Systems, LLC, shall mitigate any harmful effects on individuals whose FERC information has been accessed or disclosed in a security incident. In the event of a data breach with respect to any FERC sensitive information processed or maintained by the CSP contractor or subcontractor under the contract, the CSP contractor is responsible for damages to FERC.

3.7. ATTRIBUTES AND ACCURACY OF THE PII

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

FEMS2 captures information employees and contractors send and receive through e-mail. E-mails may contain PII. There is not a purpose or need to verify information captured by e-mail.

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

FEMS2 captures internal e-mails sent between employees, and in the event a customer or an individual of the public sends an e-mail. The information is captured and stored, but is not relied upon or necessary to be kept current. There are no decisions made that rely upon the data to be current.

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 being used?

FERC's headquarters is located at 888 First St, N.E. Washington, D.C. 20426 and is the focus of the FEMS2 system. This system is accessible by authorized users from anywhere in the world that has an Internet connection.

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

Microsoft employs the following data retention standards on data collected and maintained in the cloud on behalf of FERC.
Microsoft's data retention standards are explained in Office 365 Trust Center:

https://products.office.com/en/business/office-365-trust-center-cloud-computing-security

Microsoft contracts reflect data shown in the Trust Center, such as:

> At the end of a customer's subscription or use of the service, the customer may always export its data. Full details are contained within the Product Use Rights (which is the authoritative source on this topic), however for convenience the provisions current as of the release of Office 365 are included below:
>
> > Online Service Expiration or Termination. Upon expiration or termination of your online service subscription, you must contact Microsoft and tell us whether to:
> >
> > - (1) disable your account and then delete the customer data; or
> >
> > - (2) retain your customer data in a limited function account for at least 90 days after expiration or termination of your subscription (the "retention period") so that you may extract the data.
> >
> > - If you indicate (1), you will not be able to extract the customer data from your account. If you indicate (2), you will reimburse us for any applicable costs. If you do not indicate (1) or (2), we will retain the customer data in accordance with (2).
> >
> > - Following the expiration of the retention period, we will disable your account and then delete the customer data. Cached or back-up copies will be purged within 30 days of the end of the retention period.
>
> No Liability for Deletion of Customer Data. You agree that, other than as described in these terms, we have no obligation to continue to hold, export or return the customer data. You agree that we have no liability whatsoever for deletion of the customer data pursuant to these terms.

In addition, FERC applies the following data retention periods on emails:

General Records Schedule (GRS): 6.1-0138-2017-001, 6.1

Email Managed Under A Capstone Approach

Item	Records Description	Disposition Instruction	Disposition Authority
010	**Email of Capstone officials.** Capstone Officials are senior officials designated by account level or by email addresses, whether the addresses are based on an individual's name, title, a group, or a specific program function. Capstone officials include all those listed on an approved NARA form 1005 (NA-1005), *Verification for Implementing GRS 6.1*, and *must* include, when applicable: 1. The head of the agency, such as Secretary, Commissioner, Administrator, Chairman or equivalent; 2. Principal assistants to the head of the agency (second tier of management), such as Under Secretaries, Assistant Secretaries, Assistant Commissioners, and/or their equivalents; this includes officers of the Armed Forces serving in comparable position(s); 3. Deputies of all positions in categories 1 and 2, and/or their equivalent(s); 4. Staff assistants to those in categories 1 and 2, such as special assistants, confidential assistants, military assistants, and/or aides; 5. Principal management positions, such as Chief Operating Officer, Chief Information Officer, Chief Knowledge Officer, Chief Technology Officer, and Chief Financial Officer, and/or their equivalent(s); 6. Directors of significant program offices, and/or their equivalent(s); 7. Principal regional officials, such as Regional Administrators, and/or their equivalent(s); 8. Roles or positions that routinely provide advice and oversight to the agency, including those positions in categories 1 through 3 and 5 through 7, including: General Counsels, Chiefs of Staff, Inspectors General, etc.; 9. Roles and positions not represented above and filled by Presidential Appointment with Senate Confirmation (PAS positions); and	**Permanent.** Cut off in accordance with agency's business needs. **Item 10** - Cut off at end of appointment **Item 10** - Transfer to NARA 10 years after cutoff (Chairman and Commissioners serve 5 year appointments; equaling 15 year transfer)	DAA-GRS-2014-0001-0001

	10. Additional roles and positions that predominately create permanent records related to mission critical functions or policy decisions and/or are of historical significance. This includes those officials in an acting capacity for any of the above positions longer than 60 days. Agencies may also include individual emails from otherwise temporary accounts appropriate for permanent disposition in this category. This item *must* include all existing legacy email accounts that correlate to the roles and positions described above. If a Capstone official has more than one agency-administered email account, this item applies to all accounts. If a Capstone official has an email account managed by other staff (such as personal assistants, confidential assistants, military assistants, or administrative assistants), this item applies to those accounts. This item applies to all email regardless of the address names used by the Capstone official for agency business, such as nicknames or office title names. Email from personal or non-official email accounts in which official agency business is conducted is also included. A complete copy of these records must be forwarded to an official electronic messaging account of the officer or employee not later than 20 days after the original creation or transmission of the record. Please consult NA-1005, for more information on which positions are included within each category. Not media neutral; applies to records managed in an electronic format only. **Note 1**: Cabinet level agencies implementing a Capstone approach that includes their components/operatives must apply the above definition to each component individually. In these cases, each component/operative is considered a separate agency in terms of the above definition of Capstone Officials. A component/operative of a cabinet level agency can implement a Capstone approach independent of their department but must also conform to the entirety of this definition. **Note 2**: Smaller agencies, micro-agencies or Commissions implementing a Capstone approach may find that some of their Capstone positions fall into several of the categories above and/or that they do not have applicable roles or positions for all categories.		

011	**Email of Non-Capstone officials.** Email of all other officials, staff, and contractors not included in item 010. Not media neutral; applies to records managed in an electronic format only. **Note**: Agencies *only* using item 011 and/or item 012 of this GRS may not dispose of any email of officials in item 010, Email of Capstone Officials, of this GRS without authority from NARA in the form of another GRS or agency-specific schedule. Submission and approval of NA-1005 is still required in these instances to document those being exempted from Capstone.	**All others except those in item 012.** Includes positions and email not covered by items 010 or 012 of this schedule. This item applies to the majority of email accounts/users within an agency adopting a Capstone approach.	**Temporary.** Cut off at the end of calendar year. Delete when 10 years old, but longer retention is authorized if required for business use.	DAA-GRS-2014-0001-0002
012		**Support and/or administrative positions.** Includes non-supervisory positions carrying out routine and/or administrative duties. These duties comprise general office or program support activities and frequently facilitate the work of Federal agencies and their programs. This includes, but is not limited to, roles and positions that: process routine transactions; provide customer service; involve mechanical crafts, or unskilled, semi-skilled, or skilled manual labor; respond to general requests for information; involve routine clerical work; and/or primarily receive non-record and/or duplicative email.	**Temporary.** Cut off at the end of calendar year. Delete when 10 years old, but longer retention is authorized if required for business use.	DAA-GRS-2014-0001-0003

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?

See response to question 27 for more details about data retention.

At the conclusion of the contract, the service provider shall provide written assertion that all FERC data has been securely erased or destroyed.

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.)?

Users must authenticate to the FERC network using their government issued Personal Identify Verification (PIV) card before they can access Microsoft Outlook.

FERC uses ADFS when connecting to Office 365. This provides the Commission with the ability to set password complexity and multi-factor authentication sequences that are unique to that specific agency. This also ensures that any PII associated with the agency's users (e.g., biometrics in multi-factor authentication) are retained within that agency.

FERC uses two factor authentication for Outlook Web Access and MaaS360 for mobile access.

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?

Employees' use of a PIV card to access Microsoft Outlook does not affect individuals' privacy. The PIV card contains necessary data to grant an individual access to FERC's information systems and assures appropriate levels of security.

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

There is monitoring and tracking of e-mails, but not exclusively for access to PII.

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

N/A

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 a CSP privacy policy and is it provided to all individuals whose PII you collect, maintain or store?

Yes, the CSP has a privacy policy. However, it is the responsibility of FERC to provide a privacy policy to individuals for whom the Commission collects, maintains or stores PII. The purpose of FEMS2 is to provide messaging services to FERC employees and contractors. The possible collection or storage of PII is extraneous to the purpose and use of the system.

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

http://go.microsoft.com/fwlink/?LinkId=512132

3.11. ASSESSOR AND SIGNATURES

This Privacy Impact Assessment has been conducted by FERC and reviewed by the signatories below for accuracy.

KAVEH TAHVILDARY

Digitally signed by KAVEH TAHVILDARY
DN: c=US, o=U.S. Government, ou=Federal Energy Regulatory Commission, cn=KAVEH TAHVILDARY, 0.9.2342.19200300.100.1.1=89901001099352
Date: 2017.08.22 13:11:17 -04'00'

System Owner Signature

Name **Kaveh Tahvildary** Date Select date.

CHRISTINA HANDLEY

Digitally signed by CHRISTINA HANDLEY
DN: c=US, o=U.S. Government, ou=Federal Energy Regulatory Commission, cn=CHRISTINA HANDLEY, 0.9.2342.19200300.100.1.1=89901000210482
Date: 2017.08.17 17:23:46 -04'00'

Senior Agency Official for Privacy Signature

Name **Christina Handley** Date **8/17/2017**

4. ACRONYMS

Acronym	Definition
CSP	Cloud Service Provider
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
NIST	National Institute for Standards and Technology
OMB	Office of Management and Budget
POC	Point of Contact
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
SORN	System of Records Notice