

FedRAMP Privacy Threshold Analysis  
and Privacy Impact Assessment



FedRAMP


Distributed Solutions Inc.

AEON


Version 2.3

January 9, 2018

## Prepared by

Organization Name that prepared this document		
	Street Address	12350 Pinecrest Road
	Suite/Room/Building	Click here to enter text.
	City, State, ZIP	Reston, VA 20191

## Prepared for

Organization Name for whom this document was prepared		
	Street Address	888 1 <sup>st</sup> Street, Northeast
	Suite/Room/Building	Click here to enter text.
	City, State, ZIP	Washington, D.C. 20426

## 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
9/22/2014	1.0	All	DSI SaaS PIA/PTA	DSI
2/13/2017	2.0	All	All sections were reviewed and updated	DSI
05/18/2017	2.1	1	Change POC title and updated dates on Applicable Laws	DSI
10/30/2017	2.2	All	Small updates made throughout	DSI
11/13/2017	2.3	All	Removed CUI, Updated the Applicable Laws & Regulation and Added FERC as the agency document is prepared for, updated section 3.11 Assessor and Signatures	DSI

## 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 .....	2
1.3	Personally Identifiable Information (PII) .....	4
2	Privacy Threshold Analysis .....	4
2.1	Qualifying Questions .....	5
2.2	Designation .....	5
3	Privacy Impact Assessment .....	5
3.1	PII Mapping of Components .....	5
3.2	PII in Use .....	6
3.3	Sources of PII and Purpose .....	6
3.4	Access to PII and Sharing .....	7
3.5	PII Safeguards and Liabilities .....	8
3.6	Contracts, Agreements, and Ownership .....	10
3.7	Attributes and Accuracy of the PII .....	11
3.8	Maintenance and Administrative Controls .....	11
3.9	Business Processes and Technology .....	13
3.10	Privacy Policy .....	13
3.11	ASSESSOR AND SIGNATURES .....	13
4	ACRONYMS .....	15

## List of Tables

---

Table 1-1 - System Name Privacy POC .....	1
Table 1-2 Information System Name Laws and Regulations .....	1
Table 1-3 Information System Name Standards and Guidance .....	3
Table 3-1 PII Mapped to Components .....	5

## 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 Distributed Solutions Inc.

*Table 1-1 - System Name Privacy POC*

<b>Name</b>	Ron Falcone
<b>Title</b>	Executive Vice President
<b>CSP / Organization</b>	Distributed Solutions Inc.
<b>Address</b>	12350 Pinecrest Road, Reston, VA 20191
<b>Phone Number</b>	703-471-7530
<b>Email Address</b>	privacyofficer@distributedinc.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 is included in the System Security Plan (SSP) in ATTACHMENT 12 – FedRAMP Laws and Regulations.

Table 1-2 Information System Name Laws and Regulations include additional laws and regulations specific to **AEON**. 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 Information System Name Laws and Regulations*

<b>Identification Number</b>	<b>Title</b>	<b>Date</b>	<b>Link</b>
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>
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>
Public Law 100-503	Computer Matching and Privacy Act of 1998	October, 1998	<a href="#">5 USC 522A</a>
PL 107-347	E-Government Act [includes FISMA Title III]	December 2002	<a href="#">PL 107-347</a>
FTC	Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices	June 2008	<a href="#">FTC Sec-5</a>

Identification Number	Title	Date	Link
NARA	44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33 (see Public Law 113-187) <ul style="list-style-type: none"> <li>Ch 21 as of November 26, 2014</li> <li>Ch 29 as of November 26, 2014</li> <li>Ch 31 as of October 21, 1976</li> <li>Ch 33 as of November 16, 2014</li> </ul>	November 2014	<a href="#">NARA 44USC</a>
ECFR	Title 36, Code of Federal Regulations, Chapter XII, Subchapter B	March 2017	<a href="#">e-CFR data</a>
OMB Circular A-130	Managing Information as a Strategic Resource	7/1/2016	<a href="#">OMB A-130</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>
OMB M-17-12	Preparing and Responding to a Breach of Personally Identifiable Information.	January 2017	<a href="#">OMB M-17-12</a>
OMB M-03-22	OMB Guidance for Implementing the Privacy Provisions	September 2003	<a href="#">OMB M-03-22</a>
PL 104-191	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	August 1996	<a href="#">PL 104-191</a>
PL 108-447	Consolidated Appropriations Act of 2005, Section 522	December 2004	<a href="#">PL 100-503</a>
PL 113-187	44 U.S.C The Presidential and Federal Records Act Amendments of 2014 showing changes to NARA Statutes found below in Chapters 21, 22, 29, 31, 33, of Title 44 in PDF. <ul style="list-style-type: none"> <li>Ch 21 as of November 26, 2014</li> <li>Ch 22 as of November 26, 2014</li> <li>Ch 29 as of November 26, 2014</li> <li>Ch 31 as of October 21, 1976</li> <li>Ch 33 as of November 16, 2014</li> </ul>	December 2014	<a href="#">PL 113-187</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 is 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 Information System Name Standards and Guidance includes any additional standards and guidance specific to **AEON**. 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 Information System Name Standards and Guidance**

Identification Number	Title	Date	Link
FIPS PUB 140-2	Security Requirements for Cryptographic Modules	October 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, April 2013	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>
NIST SP 800-30	Guide for Conducting Risk Assessments, Revision 1	September 2012	<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 Applying the Risk Management Framework to Federal Information Systems	June 2014	<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]	February 2016	<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>

Identification Number	Title	Date	Link
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 Marketplace: A Federal Trade Commission Report to Congress	June 1998	<a href="#">FTC Privacy Online</a>
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 Memorandum 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

Distributed Solutions, Inc. (DSI) performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the Information System Name (Information System Abbreviation) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by DSI 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?
- No        2. Does the ISA collect, maintain, or share PII information from or about the public?
- No        3. Has a Privacy Impact Assessment ever been performed for the ISA?
- No        4. Is there a Privacy Act System of Records Notice (SORN) for this ISA system?  
If yes; the SORN identifier and name is: Enter SORN ID/Name.

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 not been conducted for the DSI SaaS. This is the first PIA for the DSI SaaS.

### 3.1 PII MAPPING OF COMPONENTS

AEON consists of Microsoft Structured Query Language (SQL) Server key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by AEON 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 PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
SQL Server	Yes (Store)	Vendor Employer Identification Number (EIN)/Taxpayer Identification Number (TIN), System for Award	FERC: Allows user to make necessary purchases from known vendor(s), associates the vendor information	FIPS 140-2 cryptography applied to specific table and table row where such data is encrypted



Components	Does this function collect or store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
		Management SAM.gov username and password	with contract award information	

### 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 Distributed Solutions, Inc. (DSI) service offering?

*DSI SaaS contains PII; however, the type of PII varies based on the Federal Energy Regulatory Commission (FERC) and the nature of the configuration of the application, which are based on customer requirements. The PII contained in the Automated Acquisition Management Solution (AAMS) is the vendor's EIN, TIN and SAM user name and password. See Table 3-1 above.*

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):

No *If and when the situation arises, DSI leaves this decision to the discretion of FERC.*

### 3.3 SOURCES OF PII AND PURPOSE

3. Does DSI have knowledge of federal agencies that provide PII to the system?

*Yes.*

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

*Yes. The purpose is stated in the agency's tailoring of security controls where NIST SP 800-53 Rev.4 requires an organizational defined setting(s).*

5. Does DSI 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.

*DSI does not have the authority to allow third party sources to provide PII to the system. DSI is unaware whether the customer receives PII from any third-party sources. The information contained in the system is what has been provided directly from the customer. See Table 3.1.*

*AAMS imports the TIN from the SAM, the official United States government system that manages data related to the peripheral acquisition systems.*

### **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?

*None. FERC has not permitted DSI to provide other Federal agencies with access to PII stored in the system.*

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

*DSI's Application Engineer(s) and SQL Administrator(s) will have access to the system and the PII, and are the staff who will need to configure the solution to capture the necessary PII, set the necessary encryption levels, test and validate the encryption and/or cryptographic module being used. There are no known contractors or other third-parties who have been given direct access to the system and/or the PII captured within the system.*

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

- With the exception of DSI's authorized personnel who are required to configure, test, and validate encryption for PII data; the criteria, procedures, controls, and responsibilities regarding access to PII data from the information system is all within the discretion and responsibility of FERC. DSI's SaaS provides role-based security where FERC is responsible for authorizing access to such data. DSI's authorized personnel are those who upon hire and based on related experience have been designated as either Application Engineers, SQL Administrators, and/or Network Engineers. In most cases, such individuals also are cleared and credentialed by agency customers in order to manage and maintain customer instance. It should be noted, however, that PII data is encrypted and therefore unviewable by network and/or SQL administrators and application engineers since the encryption and decryption happens at application level.*
- Access to the AAMS application is governed through our Financial System and Travel Staff (FSTS) Security Administration Standard Operating Procedure, which require a*

*manager's approval. Specifically, the Acquisition Services Division's Director, or their designee, is responsible for requesting all new access to the AAMS application. These initiators are also considered approving authorities and the conventional steps associated with granting access to AAMS application are listed below:*

- 1) The initiator will electronically complete the AAMS User Access Request Form. Each new access request must be accompanied by a Rules of Behavior (ROB) acknowledgement that is signed by the employee.*
- 2) The initiator emails the access request form to FSTS at: CFOsystems@ferc.gov.*
- 3) The employee will be emailed a link to the rules of behavior and must sign it electronically and send back to FSTS.*
- 4) FSTS checks the request form for completeness, correctness, and appropriateness, and works with the initiator to make any necessary changes and is also responsible for validating that the initiator is also the appropriate approving authority (Division Director or designee).*
- 5) FSTS validates that a ROB acknowledgement form has been completed, signed by the new user requesting access, and submitted to FSTS.*
- 6) Once the request package (including the AAMS User Access Request Form, the signed ROB, and any supporting email traffic) is validated, FSTS grants the documented access within the AAMS application.*
- 7) For new users, FSTS sends an email notifying the user of their ID and calls them to relay their password.*
- 8) All security documentation is archived for audit purposes.*

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?

*DSI's SaaS provides role-based security where users are either authorized and/or prohibited access to PII data pending on role assignments. FERC is solely responsible for granting access to users. Furthermore, each cloud module for FERC adheres to DSI's customized infrastructure where additional security protocols are in place to restrict access and prevent*

*misuse of PII data. Additionally, security is strengthened with the implementation of FIPS 140-2.*

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?

*The SaaS/FERC has policies and procedures for proper PII handling. In addition, DSI has its own internal policies and procedures in place for the protection of PII contained within its system.*

*In addition, FERC is responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or stored on the system. The Commission has procedures for handling PII and rules of behavior that every employee must adhere to protect the privacy rights of individuals.*

13. Does DSI's annual security training include privacy training? Does DSI require contractors to take the training?

*Yes. DSI provides annual security awareness and privacy training to its employees on at least an annual basis and upon employment. Should DSI hire any contractors, the contractor(s) will also be subject to such training.*

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

*For the infrastructure and at the security boundaries of the information system, DSI relies on Edge Hosting Commercial Cloud Service as its PaaS partner. The SaaS/FERC, with assistance from DSI, are responsible in providing a PTA and PIA that would determine the level of protection necessary for the type of PII being captured. DSI is responsible at the application level to ensure that the appropriate encryption and securities are in place to ensure safeguards for the PII are in place. In addition, DSI has its own internal policies and procedures in place for the protection of PII contained within its system.*

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 CSP or its customers could potentially be affected if an after-the-fact investigation revealed that either the CSP or the customer did not secure the system properly or sufficiently at the infrastructure/platform levels (IaaS/PaaS) or application level (SaaS/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 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 CSP or its customers could potentially be affected if an after-the-fact investigation revealed that either the CSP or the customer did not secure the system properly or sufficiently at the infrastructure or platform levels (IaaS/PaaS) or application level (SaaS/FERC). The affect or harm to the individual is dependent upon the nature of the PII the agency customers wish to have collected; therefore, agency customers will be required to perform their own privacy assessment to determine the risk and/or harm to individuals based on PII being collected.*

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?

*Contractors will not have any involvement with the design and/or maintenance of the system. DSI maintains all system components. Yes, NDAs have been developed for contractors who may work on the system. For each contractor DSI works with, all such contractors and their employees who are engaged in the project are required to sign NDAs.*

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

*Yes. DSI in its personnel policies and its engagement contracts with contractors advises PII owners that federal agencies or other organizations may require PII data and that DSI may be required to divulge such information as required. Each PII owner is also advised of DSI SaaS structure, which segregates, physically and/or 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 when applicable is covered in our contracts on an as-needed basis. As a cloud provider, Distributed Solutions Inc., (“DSI”) accepts limited liability in the event DSI fails to deliver its security services as defined in each contract. However, the contract provides that in the absence of negligence or other improper conduct the supplying organization is ultimately accountable for the security and privacy of the data supplied by it.*

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

*Yes, unless otherwise agreed to any data provided by customer in its raw form remains the property of the customer.*

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

*DSI 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. Customer's PII requirements are specified in each customer contract, and customer is obligated to notify DSI of any changes to customer's PII requirements.*

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

*Yes, DSI 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, DSI follows client directions with respect to the retention or disposal of customer data.*

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

*Yes, DSI only accepts limited liability for exposure of PII to the extent that DSI breaches the delivery of the security services contracted. However, the contract provides that in the absence of negligence or other improper conduct the supplying organization is ultimately accountable for the security and privacy of the data supplied by it.*

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

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

*This is the responsibility of the SaaS/FERC. The SaaS/FERC relies on the information collected directly from the data subject to be accurate and complete.*

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

*This is the responsibility of the SaaS/FERC.*

*Yes. FERC relies on the information it receives from the individual to be current and to notify the Commission if information submitted is inaccurate or needs to be updated.*

### **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?

*Yes. PaaS's Disaster Recovery (DR) site will have the same configuration.*

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

*This is primarily the responsibility of the SaaS/FERC in collaboration with DSI. Unless otherwise agreed to, DSI shall retain PII records for a period of three (3) years, however, with respect to client data; DSI follows client directions with respect to the retention or disposal of customer data.*

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?

*The retention period is the responsibility of the SaaS/FERC. Unless otherwise agreed to, DSI shall retain PII records for a period of three (3) years, however, with respect to client data; DSI follows client directions with respect to the retention or disposal of customer data including any PII data. As for disposition and/or sanitization (e.g. shredding, degaussing, overwriting etc.) DSI follows FedRAMP/NIST guidelines where DSI shall maintain control overall all media until a formal sanitization attestation has been requested by Customer. Upon formal request, DSI will work with a third party vendor who is licensed and approved to perform such tasks. Vendor will identify all media that has touched FERC information, which includes all primary, backup, online and off-site media. Once identification is complete and formal attestation is provided, and Vendor will use one of three (3) methods; Clear, Purge and/or Destruction for all dispositioning of data/media. The formal sanitization attestation form will outline the process and methods taken, as well as vendor information and date executed etc.*

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?

*N/A*

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

*DSI has the ability to review the Event Viewer for Windows-based systems and beyond that, the SaaS/FERC is responsible at the application layer, where audit reports can be created to see if there were any unauthorized login attempts etc. DSI's SaaS provides administrators the ability to generate reports that could verify existence of data captured as PII, but are unable to view the encrypted PII data; for example, a row within the database table set for PII may not have a "null" value.*

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

*Not applicable at this time.*

### **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?

*Yes. PIA requires the facilitation of encryption of PII information. DSI has, by default, engaged in and implemented FIPS 140-2, but will require additional and necessary configuration.*

### **3.10 PRIVACY POLICY**

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

*Yes; but DSI places the responsibilities for capturing PII to the SaaS/FERC, and therefore customer is responsible for informing individuals whose PII is collected, maintained and/or stored. In addition, DSI has its own internal policies and procedures in place for the protection of PII contained within its system.*

*FERC does not collect PII directly from the source. FERC imports the PII from SAM via AAMS. General Services Administration would be responsible for providing the required privacy notice to participate in the Central Contractor Registration program.*

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 *Federal Regulatory Commission (FERC)* and has been reviewed by the Distributed Solutions Inc., Chief Privacy Officer for accuracy.



---

FERC Senior Agency Official for Privacy

Name **Christina Handley**

Date Select date.

---

Chief Privacy Officer Signature

Name **Ron Falcone**



Date Select date.

1/30/2018

## 4 ACRONYMS

<b>Acronym</b>	<b>Definition</b>
<b>CSP</b>	Cloud Service Provider
<b>IT</b>	Information Technology
<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>PTA</b>	Privacy Threshold Analysis
<b>SORN</b>	System of Records Notice