Affects Members Of the Public? ☐

## Department of Energy

# Privacy Impact Assessment (PIA)

***Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA:*** ***https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file***

**Please complete form and return via email to Privacy@hq.doe.gov**

**No hand-written submissions will be accepted.**

**This template may not be modified.**

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | | |
|---|---|---|
| **Date** | 03/01/2023 | |
| **Departmental Element & Site** | Office of Energy Efficiency and Renewable Energy (EERE)<br><br>System managed from DOE Headquarters, 1000 Independence Ave SW, Washington DC 20585, and hosted at https://doe-eere.okta.com | |
| **Name of Information System or IT Project** | Okta for EERE | |
| **Exhibit Project UID** | UID 019-000000152 - EE Office Automation | |
| **New PIA** [X]<br>**Update** [ ] | This is a new PIA | |
| | **Name, Title** | **Contact Information Phone, Email** |
| **System Owner** | David Crouch, Management and Program Analyst | (202) 586-4844<br>David.Crouch@ee.doe.gov |

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | | |
|---|---|---|
| **Local Privacy Act Officer** | Shaida Beklik<br>EERE HQ Cyber Security Program Manager | 202-586-4769<br>Shaida.beklik@ee.doe.gov |
| **Cyber Security Expert** reviewing this document (e.g. ISSM, CSSM, ISSO, etc.) | Shaida Beklik<br>EERE HQ Cyber Security Program Manager | 202-586-4769<br>Shaida.beklik@ee.doe.gov |
| **Person Completing this Document** | Adam Giannini,<br>EERE HQ Cyber Security Support | (571) 406-5940<br>Adam.giannini@ee.doe.gov |
| **Purpose of Information System or IT Project** | The Okta Identity as a Service (IDaaS) FedRAMP Platform makes it easy for customers to authenticate, manage and secure their users. Okta's Platform products include Universal Directory, Single Sign-On, Provisioning, Adaptive Multi-factor Authentication, Social Authentication, Inbound Federation, Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) Integration. The Okta IDaaS system offers a complete identity and access solution addressing the needs of IT Operations, End Users, and Business Leaders with no customization required.<br><br>EERE utilizes Okta's Single Sign-On and Universal Directory services, which include password management functionality. Okta is not integrated with EITS Active Directory. It is strictly used to manage passwords and provide single sign on capabilities with various web applications such as Webex, Learning Nucleus, Zoom etc. Okta IDaaS is a FedRAMP-Authorized SaaS cloud provider operating at the Moderate baseline.<br><br>Okta IDaaS FedRAMP secures the underlying infrastructure of the Okta Identity Cloud Platform. EERE has configured their instance of Okta to secure the information stored by users. A security white paper has been published by Okta and is available for system administrators to reference. EERE is only using Okta's Single Sign-On and Universal Directory services.<br><br>The Okta service is accessed by approximately 150 EERE users, consisting of both Federal employees and contractors at EERE HQ, Golden Field Office and the Office of the Inspector General.<br><br>The service is accessed at https://doe-eere.okta.com. | |
| **Type of Information Collected or Maintained by the System**: | ☐ SSN Social Security number<br><br>☐ Medical & Health Information e.g. blood test results | |

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| | ☐ Financial Information e.g. credit card number<br>☐ Clearance Information e.g. "Q"<br>☐ Biometric Information e.g. finger print, retinal scan<br>☐ Mother's Maiden Name<br>☐ DoB, Place of Birth<br>☐ Employment Information<br>☐ Criminal History<br>☒ Name, e-mail address (Business Contact Information, optional address, optional phone number)<br>☐ Other – Please Specify<br><br>One of Okta's functions is as a password / credential manager. Users can input any information into this part of the application, including address/phone number. There is no way to control what is input in here. For the creation of Okta accounts, however, only name and email address are required/used for provisioning the account. Phone number or address (business or otherwise) are OPTIONAL and not required for access to the system. |
| **Has there been any attempt to verify PII does not exist on the system?**<br><br>**DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.* | No; PII is knowingly collected. |
| **If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)** | PII will be collected by the application and stored within the system. |

## Threshold Questions

| | |
|---|---|
| **1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?** | YES |

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| **2. Is the information in identifiable form?** | YES |
| **3. Is the information about individual Members of the Public?** | NO |
| **4. Is the information about DOE or contractor employees?** | YES<br>☒ Federal Employees<br>☒Contractor Employees |

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

**Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.**

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

# END OF PRIVACY NEEDS ASSESSMENT

# MODULE II – PII SYSTEMS & PROJECTS

## AUTHORITY, IMPACT & NOTICE

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **1. AUTHORITY**<br>**What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?** | Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 et. seq.<br>2 Code of Federal Regulations (C.F.R.) 200, as amended by 2 C.F.R. Section 910 |
| **2. CONSENT**<br>**What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?** | Users must provide a name and business e-mail address to use the system. By providing name and business e-mail to use this system, users consent to this information being collected. Users are given the opportunity to decline having their account created if they do not wish to have this information collected. |
| **3. CONTRACTS**<br>**Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?** | Currently, only Federal staff administers the application for EERE.<br><br>This is a FedRAMP authorized cloud service, therefore, there are non-Federal personnel involved with the design, development, and maintenance of the system. |
| **4. IMPACT ANALYSIS:**<br>**How does this project or information system impact privacy?** | Okta for EERE does not collect/maintain sensitive PII, like SSN or date of birth, which limits the privacy impact. If the system or data is breached, the impact to the individual's privacy would be low since the PII maintained in the system is basic business contact information (name and email address).<br><br>Okta for EERE is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls:<br><br>• Strict access control enforcement based on need-to-know |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **5. SORNs**<br>**How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?**<br>**If yes, explain, and list the identifiers that will be used to retrieve information on the individual.** | The names and email addresses of users can be viewed by system administrators but are otherwise unable to be retrieved. |
| **6. SORNs**<br>**Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?**<br>**If "Yes," provide name of SORN and location in the *Federal Register*.** | N/A, PII is not retrievable by an identifier (e.g., name, unique number or symbol), see #5 above. |
| **7. SORNs**<br>**If the information system is being modified, will the SORN(s) require amendment or revision?** | N/A |
| **DATA SOURCES** | |
| **8. What are the sources of information about individuals in the information system or project?** | Users provide their own contact information (name and email address). |
| **9. Will the information system derive new or meta data about an individual from the information collected?** | No. The system will not derive new or meta data about an individual from the information collected. |
| **10. Are the data elements described in detail and documented?** | Yes. |
| **DATA USE** | |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **11. How will the PII be used?** | The user's email address is used to login to the system. The user's name is associated with the account. |
| **12. If the system derives meta data, how will the new or meta data be used?**<br>**Will the new or meta data be part of an individual's record?** | N/A. No meta data is derived by the system. |
| **13. With what other agencies or entities will an individual's information be shared?** | No information will be shared with other agencies, entities, or third-parties. |
| **Reports** | |
| **14. What kinds of reports are produced about individuals or contain an individual's data?** | Only system usage/audit reports are generated. System administrators can generate a report with last login date for users of the system. |
| **15. What will be the use of these reports?** | The reports are used to determine if inactive accounts exist and should be deactivated. |
| **16. Who will have access to these reports?** | The reports are available only to system administrators (currently only the Okta for EERE system owner). |
| **Monitoring** | |
| **17. Will this information system provide the capability to identify, locate, and monitor individuals?** | No. |
| **18. What kinds of information are collected as a function of the monitoring of individuals?** | N/A. No information is collected as a function of monitoring individuals. |
| **19. Are controls implemented to prevent unauthorized monitoring of individuals?** | Yes. Although the site/system does not have monitoring capability, EERE has implemented security controls to prevent unauthorized users from monitoring or accessing any of the PII on the system (e.g., Access Controls). |
| **DATA MANAGEMENT & MAINTENANCE** | |

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.** | Contact information for individuals is input by the Okta for EERE system administrator at time the individual's account is created. If a user needs to update their contact information, they may login to their account to do so. |
| **21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?** | Okta for EERE is a Software as a Service (SaaS) delivery model supported by the Amazon Web Services infrastructure. All authorized users access the system through a web browser. |
| **Records Management** | |
| **22. Identify the record(s).** | System access records (login files, contact information, system usage, and audit reports). |
| **23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.** | Check appropriately and cite as required.<br><br>☐ Unscheduled X Scheduled *(cite NARA authority(ies) below)*<br><br>**System Access Records**<br>• Systems requiring special accountability for access. GRS 3.2, item 030 (DAA-GRS-2013-0006- 0003) Temporary. Destroy when business use ceases. |
| **24. Records Contact** | Tia Alexander<br>Tia.Alexander@ee.doe.gov<br>202-586-3135 |
| **ACCESS, SAFEGUARDS & SECURITY** | |
| **25. What controls are in place to protect the data from unauthorized access, modification or use?** | The provider of the system, Okta IDaaS has numerous policies, practices, and technologies in place that complement DOE's controls for protecting data. These include contractual safeguards, codes of conduct, employee training on privacy and security issues, invisibility of customer passwords, and firewalls and intrusion detection around the hosting center. |
| **26. Who will have access to PII data?** | Based on Okta for EERE system's permissions model and access level, designated System Administrators (currently only the System Owner) will have access to PII data to perform their duties. |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **27. How is access to PII data determined?** | Based on Okta for EERE's permissions model and access level, designated System Administrators (currently only the System Owner) will have access to PII data to perform their duties. |
| **28. Do other information systems share data or have access to the data in the system? If yes, explain.** | No outside information systems have access to this data |
| **29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?** | N/A -There are no interconnected systems. |
| **30. Who is responsible for ensuring the authorized use of personal information?** | System Owner.<br><br>The only information about an individual that can be accessed by the system owner is the name and email address of that user. Accounts are disabled for users that are inactive for 60 days or more. If a user leaves the department or otherwise no longer require access moving forward, their account (and information) is deleted and removed from the system. |
| **END OF MODULE II** | |

| SIGNATURE PAGE | | |
|---|---|---|
| | **Signature** | **Date** |
| **System Owner** | David A. Crouch<br>Digitally signed by David A. Crouch<br>Date: 2023.10.31 13:43:00 -04'00'<br>**(Print Name)**<br>**(Signature)** | |
| **Local Privacy Act Officer** | Shaida Beklik<br>Digitally signed by Shaida Beklik<br>Date: 2023.10.31 13:30:51 -04'00'<br>**(Print Name)**<br>**(Signature)** | |
| ***Ken Hunt***<br>**Chief Privacy Officer** | William K. Hunt<br>Digitally signed by William K. Hunt<br>Date: 2023.10.27 13:51:16 -04'00'<br>**(Print Name)**<br>**(Signature)** | |