Affects Members Of the Public? X

## Department of Energy

Privacy Impact Assessment (PIA)

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| **Date** | 1/30/24 |
| **Departmental Element & Site** | Office of the Chief Information Officer<br>Cybersecurity Compliance and Oversight Office, IM-50<br>U.S Department of Energy |
| **Name of Information System or IT Project** | MyEnergy |
| **Exhibit Project UID** | N/A |
| **New PIA** ☐<br>**Update** x | Update to clarify PII stored in the system. |

| | Name, Title | Contact Information Phone, Email |
|---|---|---|
| **System Owner** | Johnny Dicus<br>System Owner | 208-526-0847<br>johnny.dicus@hq.doe.gov |
| **Local Privacy Act Officer** | Brooke Dickson<br>Privacy Management and Compliance Officer /DOE IM-42 | 202-287-5786<br>brooke.dickson@hq.doe.gov |
| **Cyber Security Expert** reviewing this document (e.g. ISSM, CSSM, ISSO, etc.) | Charlene Kamadeu<br>IM50's Information System Security Officer<br>(ISSO) | Charlene Kamadeu<br>510-759-5624<br>charlene.kamadeu@hq.doe.gov |
| **Person Completing this Document** | Charlene Kamadeu<br>IM50's Information System Security Officer | Charlene Kamadeu<br>510-759-5624<br>charlene.kamadeu@hq.doe.gov |

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | | |
|---|---|---|
| | (ISSO). | |
| **Purpose of Information System or IT Project** | MyEnergy.gov is a Department of Energy (DOE) Office of the Chief Information Officer (OCIO) cloud-based solution that supports user login as part of compliance with the 21st Century Integrated Digital Experience Act (IDEA) Act. MyEnergy.gov enables designated users to digitize, manage, interface with, conduct data entry for, digitally sign, and route a defined series of Departmental forms in accordance with the IDEA Act mandate. In the production environment we have the following forms:<br>• *DOE F 231.5*<br>• *HC Telework Form*<br>• *HC Remote work Form*<br>• *GDO Solar Application Forms*<br>• *Certification of Vaccination-DOE Onsite Contractor Employees*<br>• *Verification Vaccination Form*<br>• *PR-ERF Household Intake Form*<br>In addition to the forms in the production environment, users will be able to access the following custom applications and service portals supporting various DOE business processes:<br>• *MyEnergy* - Provides web-based forms with digital / electronic signatures.<br>• *Human Capital Portal* - Provides for Federal staffing and classification.<br>• *BIL NEPA Portal* - Provides tracking of bipartisan legislation for NEPA funding.<br>• *GDO Solar* - Provides applications and tracking lifecycle of GDO Solar applications.<br>MyEnergy.gov will serve as a user access portal, providing a landing site for form accessibility and user access control for single-sign-on (SSO) access for both public and DOE users via DOE OneID (PIV for DOE users and ID.me for public users).<br>ServiceNow Government Community Cloud (FedRAMP High, Package ID F1305072116) provides MyEnergy.gov as an integrated Platform-as-a-Service (PaaS) as well as a Software-as-a-Service (SaaS) offering to DOE, classified as a FISMA Moderate system. MyEnergy.gov is a public-facing system. Users may access the system using either a public persona, for which they must establish a proofed-based (IAL2) identity with ID.me, or a DOE persona, in which case they must use their PIV card both authentication happens through DOE's OneID identity provider. ID.me is intergraded with OneID. SAMLv2 is the authentication protocol used by OneID when authenticating for MyEnergy.gov. | |

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| | MyEnergy tokenizes personally identifiable information (PII) users put into forms to increase privacy protection and minimize risk. Tokenization substitutes PII with surrogate values called tokens, which can then be used to represent the original (or raw) sensitive value. PII is further protected by access control lists (ACLs) limiting access to ServiceNow administrators based on a need-to-know.<br><br>The public persona protocol functions as follows: public users will go to the portal and choose ID.me. They will be redirected to ID.me site where they will be prompted to create an account and ID proofing. For example, a public user may use their driver's license as proof as well as credit bureau and cell service provider. The ID.me site has the user upload a picture and then proofs the user. Once the account is created they will be taken back to MyEnergy where they will then have access to the forms via one OneID. |
| **Type of Information Collected or Maintained by the System**: | ☒ Social Security number<br>☒ Medical & Health Information<br>☒ Financial Information<br>☐ Clearance Information<br>☐ Biometric Information<br>☒ Mother's Maiden Name<br>☒ DoB, Place of Birth<br>☐ Employment Information<br>☐ Criminal History<br>☒ Name, Phone, Address<br>☒ Other – (information on the Puerto Rico Energy Resilience Fund household intake form<br><br>1) Household data to include Street, apt/house #, Municipality, Latitude, Longitude<br><br>2) Name of Homeowner (paternal Last Name, Maternal last Name), Homeowner Phone, Alternate Phone, Homeowner email address, energy dependent disability (if applicable). |

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| | 3) PII from documents such as Proof of Low-income Home Energy Assistance Program, Nutrition Assistance Program, or Temporary Assistance for Needy Families. Photo of electrical medical device, Letter from Social Security, Medicare, Medicaid, Veteran Affairs, Copies of property deed, Copy of notarized affidavit of ownership, Property tax receipts, Utility bills. |
| **Has there been any attempt to verify PII does not exist on the system?**<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.* | PII exists. |
| **If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)** | N/A. |

## Threshold Questions

| | |
|---|---|
| **1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?** | YES |
| **2. Is the information in identifiable form?** | YES |
| **3. Is the information about individual Members of the Public?** | YES |
| **4. Is the information about DOE or contractor employees?** | YES<br>☒ Federal Employees<br>☒ Contractor Employees |

# END OF PRIVACY NEEDS ASSESSMENT

# MODULE II – PII SYSTEMS & PROJECTS

## AUTHORITY, IMPACT & NOTICE

| | |
|---|---|
| **1. AUTHORITY**<br>**What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?** | • 42 U.S.C. § 7101 et seq.<br>• 5 U.S.C. § 552a<br>• 10 CFR § 1008 |
| **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)?** | Individuals have the opportunity and/or right to decline to provide Information. |
| **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?** | Yes. Contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need-to-know basis. Contractors are required to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel. |

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **4. IMPACT ANALYSIS:**<br>**How does this project or information system impact privacy?** | DOE has assessed MyEnergy as a moderate-risk system according to the criteria set forth in Federal Information Processing Standard (FIPS) 199 established by the National Institute of Standards and Technology (NIST). The risk rating is used to determine the effect to the agency should the system's confidentiality, integrity or availability be compromised.<br><br>The unauthorized disclosure of information is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. MyEnergy holds some sensitive PII, e.g., SSN. If PII maintained in this system were disclosed to unauthorized parties, the sensitivity there of could compromise trust between employees and the employer and cause embarrassment or harm to the individual whose information was exposed. The breach of SSNs would result in the most serious potential harm to individuals posed by MyEnergy. In addition, information respecting foreign influence determinations may also adversely impact the privacy of individuals resulting in reputational harm via association with the organization being assessed.<br><br>The system Implements the Fair Information Practice Principles (FIPPs) through a series of controls and processes in place to ensure that controls are operating effectively to mitigate the risk of MyEnergy being compromised. PII is minimized to what is needed for authorized, specified business purposes and is not used for unauthorized or additional purposes. The System Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. PII in MyEnergy ServiceNow is housed on secure servers that are encrypted at rest and in transit by the FEDRAMP-approved ServiceNow Cloud. All instances within the ServiceNow platform have Full Disk Encryption enabled. Access to data is controlled and limited to MyEnergy system administrators. PII in MyEnergy is tokenized and kept in a token/value pair table that has access controls limited to MyEnergy system administrators. The system was certified and accredited and found to have mitigated risk to an acceptable level. |

| 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.** | PII is not retrieved in practice by name or unique identifier. |
| **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*.** | Any PII retrievals would be covered under OPM/GOVT-1 and DOE-82, 74 FR 1082. |
| **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?** | Individuals input their PII into MyEnergy when filling out the forms listed in the purpose section. |
| **9. Will the information system derive new or meta data about an individual from the information collected?** | No. |
| **10. Are the data elements described in detail and documented?** | See System Security Plan. |
| **DATA USE** | |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **11. How will the PII be used?** | PII is used in accordance with the purposes relating to the forms listed in the Purpose section. MyEnergy has a REST web service which Adobe calls to "tokenize" a PII field. Adobe sends the SSN, MyEnergy "tokenizes" it and sends back the token so Adobe can request it via REST interface and MyEnergy sends back (over SSL REST response) the PII. While at rest on the MyEnergy ServiceNow instance, this information is kept in a token/value pair table that has access controls limited to MyEnergy system administrators. When the document is completed and needs to be distributed (via email), MyEnergy receives the completed document (which may have PII in clear text) as an email. MyEnergy will then distribute this email (i.e., re-send) to the appropriate people as per the workflow for that form. Once the email has been distributed, it is marked as eligible for deletion. MyEnergy has a scheduled job which can be configured to run at any frequency which then removes these documents from MyEnergy. Removal is currently set for 24 hours. |
| **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 |
| **13. With what other agencies or entities will an individual's information be shared?** | PII will not be shared with other agencies or individuals. |
| **REPORTS** | |
| **14. What kinds of reports are produced about individuals or contain an individual's data?** | MyEnergy does not produce reports containing PII. |
| **15. What will be the use of these reports?** | N/A. |
| **16. Who will have access to these reports?** | N/A. |
| **MONITORING** | |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **17. Will this information system provide the capability to identify, locate, and monitor individuals?** | MyEnergy does not provide monitoring capabilities beyond what is self evident in the PII users put into the system, e.g., address. |
| **18. What kinds of information are collected as a function of the monitoring of individuals?** | N/A. |
| **19. Are controls implemented to prevent unauthorized monitoring of individuals?** | Security controls have been implemented and processes are in place to ensure that controls are operating effectively to mitigate the risk of MyEnergy being compromised. The System Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. PII in MyEnergy is tokenized and kept in a token/value pair table that has access controls limited to MyEnergy system administrators. The system was certified and accredited and found to have mitigated risk to an acceptable level. ServiceNow information is housed on secure servers that are encrypted at rest and in transit by the FEDRAMP-approved ServiceNow Cloud. All instances within the ServiceNow platform have Full Disk Encryption enabled. |
| **DATA MANAGEMENT & MAINTENANCE** | |
| **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.** | Adobe sends the PII, then MyEnergy "tokenizes" it and sends back the token so Adobe can request it via REST interface and MyEnergy sends back (over SSL REST response) the PII. The PII has already been verified by Adobe. |
| **21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?** | N/A. |
| **RECORDS MANAGEMENT** | |
| **22. Identify the record(s).** | Audit Records (GRS 3.2, item 030)<br>Access Control Records (GRS 3.2, item 030) |
| **23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.** | Records are scheduled under DAA-GRS2013-0006-0003 |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **24. Records Contact** | Maria Levesque – IM-41<br><br>Maria.Levesque@hq.doe.gov |
| **ACCESS, SAFEGUARDS & SECURITY** | |
| **25. What controls are in place to protect the data from unauthorized access, modification or use?** | The System Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. PII in MyEnergy ServiceNow is housed on secure servers that are encrypted at rest and in transit by the FEDRAMP-approved ServiceNow Cloud. All instances within the ServiceNow platform have Full Disk Encryption enabled. Access to data is controlled and limited to MyEnergy system administrators. PII in MyEnergy is tokenized and kept in a token/value pair table that has access controls limited to MyEnergy system administrators. The system was certified and accredited and found to have mitigated risk to an acceptable level. |
| **26. Who will have access to PII data?** | System Administrators |
| **27. How is access to PII data determined?** | Access to PII is provided exclusively on a need-to-know basis. |
| **28. Do other information systems share data or have access to the data in the system? If yes, explain.** | No. |
| **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 |

# SIGNATURE PAGE

| | Signature | Date |
|---|---|---|
| *Johnny Dicus*<br>**System Owner** | **Johnny Dicus**<br>**(Print Name)**<br>JOHNNY DICUS Digitally signed by JOHNNY DICUS Date: 2024.04.23 10:56:27 -04'00'<br>**(Signature)** | |
| **Local Privacy Act Officer** | **Brooke Dickson**<br>**(Print Name)**<br>William K. Hunt Digitally signed by William K. Hunt Date: 2024.04.22 11:03:24 -04'00'<br>**(Signature)** | |
| *Ken Hunt*<br>**Chief Privacy Officer** | **William K. Hunt**<br>**(Print Name)**<br>William K. Hunt Digitally signed by William K. Hunt Date: 2024.04.22 11:03:36 -04'00'<br>**(Signature)** | |