Affects Members Of the Public? X

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	September 13, 2022
Departmental Element & Site	Office of Environment Health, Safety and Security Office of Headquarters Security Operations Office of Physical Protection Room 1G-024B, DOE Forrestal and Room A-070, DOE Germantown
Name of Information System or IT Project	Headquarters Access Control, IPVideo, and Visitor Management System (HACS)
Exhibit Project UID	019-10-01-22-01-8062
New PIA ☐ **Update** X	This is periodic update of the HACS PIA dated April 19, 2021. No material changes to the system.

	Name, Title	Contact Information Phone, Email
System Owner	Marc Smith Office of Physical Protection Office of Headquarters Security Operations EHSS-41	Marc Smith 202-586-4441 Marc.Smith@hq.doe.gov
Local Privacy Act Officer	Raymond Holmer Office of Information Management, EHSS-72	(301) 903-7325 Raymond.Holmer@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Andrew Snow Edgewater Federal Solutions Office of Information Management, EHSS-72	703-789-6385 Andrew.Snow@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Person Completing this Document	Steve Heineman Contractor to Office of Headquarters Security Operations, EHSS-41	301-903-0293 Steve.Heineman@hq.doe.gov
Purpose of Information System or IT Project	HACS supports the Office of Physical Protection by providing ProForce officers the ability to monitor and control access as well as physical intrusion detection capabilities for Department of Energy (DOE) Headquarters (HQ) facilities and classified areas. Headquarters security staff input information into the access control system, including name, likeness, birthdate, physical identifiers (height, weight, hair/eye color), and security clearance level. All badge recipients submit enrollment forms through the Office of Personnel Security before processing in the access control system. HACS uses this information to authenticate badge holders to access the Headquarters building entrances and security areas within the buildings. Additionally, HACS provides a self-service visitor Kiosk for those with active HSPD-12 credentials from other government agencies (OGA). The Kiosk collects name, likeness, issuing agency, and fingerprint to verify identity. HACS also provides closed circuit live and archived video from security cameras throughout Headquarters. Headquarters Security Visitor Management System (HSVMS) allows EHSS-41 to register and record all visitors to the Germantown, Forrestal, and Portals buildings. HSVMS records name, image, self-reported employer, and citizenship. The system allows for a paper badge to be printed and scanned when the visitor enters and leaves the building. Access granted by the visitor system is good only the day issued and does not provide electronic access to any entrance or security area.	
Type of Information Collected or Maintained by the System:	☐ SSN ☐ Medical & Health Information ☐ Financial Information ☒ Clearance Information ☐ Biometric Information ☐ Mother's Maiden Name ☒ DoB, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address	

MODULE I – PRIVACY NEEDS ASSESSMENT

	☒ Other – Facial image, height, weight, hair color, eye color, driver's license number, citizenship, clearance level
Has there been any attempt to verify PII does not exist on the system? **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 on the system.
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 ☒ Federal Employees ☒ Contractor Employees

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **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
2. CONSENT **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)?**	Information is provided voluntarily by individuals wishing to gain access to DOE Headquarters facilities. Individuals may decline to provide their information and may be accordingly denied access.
3. CONTRACTS **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?**	DOE contractors are involved with the design, development, and maintenance of the system. Privacy Act contract clauses and other regulatory measures are addressed in their contracts. Section 13 of the contracts, *Protection of Federal Personally Identifiable Information (PII)*, states the contractors' obligations to protect PII under the Privacy Act.

MODULE II – PII SYSTEMS & PROJECTS	
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	HACS contains low sensitivity PII including basic biographic and contact information and moderately sensitive PII including employment information, clearance information, and biometric information. Should PII in the system be compromised, it could result in a moderate adverse impact to individuals. Should employment and clearance information be compromised, the compromise could cause personal harm to individuals including embarrassment and professional harm should negative information relating to individuals' clearance or access be viewed without authorization. HACS observes a number of protections to protect privacy via the Fair Information Practice Principles (FIPPs). HACS maintains the minimum PII necessary for its business purpose to mitigate privacy harm. In addition, use of the PII in HACS is limited to clearly defined business purposes. Access to and use of PII in the system is protected by a series of controls including role and permission-based monitoring controls and periodic auditing with penalties in place should mishandling of PII be discovered. System logs and auditing ensure the accuracy and currency of PII in the system.
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	Data may be retrieved by name or badge number of subject individual. The system is designed to track subject individuals' access within the facilities it monitors.
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	DOE-51 Employee and Visitor Access Control Records, 74 FR 1053

MODULE II – PII SYSTEMS & PROJECTS	
7. SORNs **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 provide the information during the badging process.
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?	Yes, data elements are described in the system help files and documented in the operations manual. Additionally, the HACS database provides a view of the scheme.
DATA USE	
11. How will the PII be used?	PII is used to identify subject individuals who have been approved to enter DOE HQ facilities.
12. If the system derives meta data, how will the new or meta data be used? **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?	Records from this system will not be shared with other agencies beyond the routine uses set forth in DOE-51.
REPORTS	

MODULE II – PII SYSTEMS & PROJECTS

14. What kinds of reports are produced about individuals or contain an individual's data?	HACS produces an access list which provides the names of individuals authorized access to an area. This type of report can be based on the individual or the area. If it is based on an individual, it will identify what areas of access the person has. If it is based on area, the list will detail all individuals who have access to a given area and what privileges they have. These reports are provided to verify the individuals who have access to an area, or to verify that a person has all of the access privileges they are supposed to have. The system administrators are the only ones who can produce these reports and they are generated as needed to help maintain access control based on the requirements of the responsible security officer for the area in question. HACS produces an individual activity report to determine where an individual has used the system. The system administrators are the only ones who can generate this type of report. It is normally generated as a troubleshooting aid to validate reports of system problems and identify a cause. This report can also be generated at the request of authorized law enforcement or security officials. The Visitor Management system can generate reports of dates and times visitors enter and leave the buildings. These reports contain visitor names, dates and times of entry/exit, lobby entered, employer reason for visit, and the name of the DOE contact. Only HACS administrators and ProForce management can generate these reports and they are considered CUI unless authorized by EHSS federal oversight for distribution (e.g., FOIA requests). All reports are treated as sensitive information. They are retained only as long as necessary in accordance with the records schedule and are designated for destruction as soon as they are no longer needed.
15. What will be the use of these reports?	See 14. Above.
16. Who will have access to these reports?	The system administrators will have access to view and modify all data in the system. Other HACS personnel will have access to view data in the system but can only modify the identification information.
MONITORING	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes, as a function of system design and purpose.

MODULE II – PII SYSTEMS & PROJECTS	
18. What kinds of information are collected as a function of the monitoring of individuals?	Access lists provide the names of individuals authorized access to an area. This type of report can be based on the individual or the area. If it is based on an individual, it will tell what areas the person has access to. If it is based on area, the list will detail all individuals who have access to a given area and what privileges they have. Individual activity reports are produced to determine where an individual has used the system. Additionally, the visitor management system collects data about individuals' entry and exists through the HQ building public lobbies.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Yes. Administrative controls are in place to inform users of the authorized uses of the system and its data. System logs record user activity and are reviewed on a periodic basis, by the system administrators, for inappropriate activities, in accordance with DOE HQ policy and procedures. Misuse of the data is subject to administrative actions up to and including dismissal. Administrators and System Administrators by virtue of managing the entire system have access to all data on the system.
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.	Data will be reviewed by the badge office personnel at the time of data entry. The system requires all data elements to be completed before the transaction can be successfully completed. Data is re-verified when badges expire, and the person is re-enrolled.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The system is operated at the DOE Headquarters facilities. Consistent use of the system and data is maintained by training in the use of the system and an annual security refresher. Administrative practices and controls are in place to ensure consistent use of the system and data at all sites. Data consistency is maintained by having the data reside at only one location. All updates are made to the same instance of the database. Any change to data forces the system to refresh data stored on field panels.
RECORDS MANAGEMENT	
22. Identify the record(s).	Security administrative records, visitor processing records, local facility identification and card access records.

MODULE II – PII SYSTEMS & PROJECTS	
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	GRS 5.6, Items 010, 110, 111, or 130
24. Records Contact	Baldev Dhillon, 301-903-0990
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Administrative and technical controls prevent unauthorized use of and access to PII. System logs record user activity and are reviewed on a periodic basis by the system administrators for inappropriate activities in accordance with DOE HQ policy and procedures. System privilege restrictions are in place to reduce the number of individuals who have access to data in the system. All personnel with access to data in the system receive training and are made cognizant of security, privacy, and confidentiality requirements involved with handling, protecting, and properly disposing of such information. Misuse of data in the system is subject to administrative actions up to and including dismissal.
26. Who will have access to PII data?	System administrators will have access to view and modify all data in the system. Other HACS personnel can view data in the system but can only modify identification information. Information in the system may be disclosed as part of the routine uses enumerated in DOE-51.
27. How is access to PII data determined?	User profiles are established and roles are defined for those profiles. Roles determine which users see which data. The system owner determines which individuals have access through user profiles. Access to data is on a need-to-know basis in accordance with the job roles and responsibilities of the individual. When a user's employment is terminated or transferred, system access privileges are terminated. Criteria, procedures, controls, and responsibilities are documented in the system security plan.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No.

MODULE II – PII SYSTEMS & PROJECTS	
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
30. Who is responsible for ensuring the authorized use of personal information?	The system owner is responsible for assuring proper use of the data. Data is generally not shared with other agencies.
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	_____Marc Smith_____ **(Print Name)** Marc D. Smith Digitally signed by Marc D. Smith Date: 2022.11.28 07:12:14 -05'00' _____ **(Signature)**	_____
Local Privacy Act Officer	_____Raymond Holmer_____ **(Print Name)** RAYMOND HOLMER Digitally signed by RAYMOND HOLMER Date: 2022.11.30 15:45:29 -05'00' _____ **(Signature)**	_____
Ken Hunt **Chief Privacy Officer**	_____ **(Print Name)** Brooke J. Dickson Digitally signed by Brooke J. Dickson Date: 2022.11.23 09:25:14 -05'00' _____ **(Signature)**	_____