Affects Members Of the Public? ☐

**Department of Energy**

# Privacy Impact Assessment (PIA)

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| **Date** | July 20, 2022 |
| **Departmental Element & Site** | SC/BNL |
| **Name of Information System or IT Project** | C-Cure Access System |
| **Exhibit Project UID** | DE-SC0012704 |
| **New PIA** ☐ **Update** X | This is an update to the C-Cure Access System PIA. |

| | Name, Title | Contact Information Phone, Email |
|---|---|---|
| **System Owner** | Robert Gordon, Brookhaven Site Manager<br>Virgilio Martinez, Security Operations Manager | (631) 344-3346<br>Robert.Gordon@science.doe.gov<br>(631) 344-4691<br>jmartinez@bnl.gov |
| **Local Privacy Act Officer** | Miriam Bartos,<br>FOIA/Privacy Act Officer | (630) 252-2041<br>Miriam.Bartos@science.doe.gov |
| **Cyber Security Expert** reviewing this | Ian Ballantyne, Information Systems Security Manager | (631) 344-7589<br>ballant@bnl.gov |

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | | |
|---|---|---|
| document (e.g. ISSM, CSSM, ISSO, etc.) | | |
| **Person Completing this Document** | Christine Metz, BNL Privacy Officer | (631) 344-2180<br>cmetz@bnl.gov |
| **Purpose of Information System or IT Project** | The C-Cure Access System (CCure) provides control and permissions for access to protected/sensitive areas across Brookhaven National Laboratory (BNL). Access to this area is only granted by persons with proper authority, such as secure area managers and senior department/division officials. CCure provides access permissions which implement system restrictions based on need-to-know protocols. An identification badge is provided for physical security access control.<br>CCure contains limited PII used to maintain the safety and security of BNL facilities and personnel, including name, employment information, site access permission, and Life Number. 'Life Number' refers to a unique number issued to BNL employees for life, used to assign benefits and for training purposes. | |
| **Type of Information Collected or Maintained by the System**: | ☐ SSN<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 (Department only)<br>☐ Criminal History<br>☒ Name, Phone, Address (Name only)<br>☒ Other – Please Specify (Site Access Permission, Citizenship, life number) | |
| **Has there been any attempt to verify PII does not exist on the system?** | | N/A. This system is designed to collect and maintain PII. |

# MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| **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.* | |
| **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?** | NO |
| **4. Is the information about DOE or contractor employees?** | ☒ 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?** | • Department of Energy Organization Act of 1977 (42 U.S.C. 7101 et seq.)<br>• Title 5, Code of Federal Regulations (CFR), Parts 5 and 736. |
| **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 voluntarily provide personal information as a necessary term of employment or other relational arrangement with BNL with notice that the information will be used for the management and security of BNL. Should an individual decline to provide the information, employment or other arrangement requiring access to protected areas within BNL may not proceed. |
| **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, under contract BNL Prime Contract, No. DE-SC0012704, under clause H.8 Privacy Act Records. |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **4. IMPACT ANALYSIS:**<br>**How does this project or information system impact privacy?** | A compromise of PII in the system could have a moderate-to-severe impact on organizational operations, organizational assets, or individuals. Should related to employment, access, or citizenship be compromised, it could result in professional or financial harm to individuals which could in turn result in personal or social harm. Should site access information be compromised, it could threaten the security of BNL facilities and personnel with potentially severe consequences. A compromise of data in CCure would potentially seriously damage the trust between BNL personnel and their employer.<br><br>CCure observes a number of protections to protect privacy via the Fair Information Practice Principles (FIPPs). CCure maintains the minimum PII necessary for its business purpose to mitigate privacy harm. In addition, use of the PII in CCure 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. The Laboratory Protection Division actively ensures the accuracy and currency of PII in the system via auditing as outlined in ID Badging Procedure (PS-2). In addition, system protections take into account NIST SP 800-53 guidelines to minimize privacy impacts. |
| **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.** | Site access permissions and activity may be retrieved by unique identifier by personnel with a use authorization and a need to know. |
| **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*.** | DOE-63, Personal Identity Verification, 74 FR 1068, January 9, 2009 |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **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?** | All data is provided by the individual. |
| **9. Will the information system derive new or meta data about an individual from the information collected?** | No. The information system will not derive new or meta data. |
| **10. Are the data elements described in detail and documented?** | A database schema exists for all data stored in CCure. |
| **DATA USE** | |
| **11. How will the PII be used?** | Data will be used to authorize Physical Security Access. |
| **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 - The system does not derive meta data. |
| **13. With what other agencies or entities will an individual's information be shared?** | None. |
| **REPORTS** | |
| **14. What kinds of reports are produced about individuals or contain an individual's data?** | Clearance Access and Activity Logs. |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **15. What will be the use of these reports?** | To inform security personnel and BNL management on clearance access activity. |
| **16. Who will have access to these reports?** | Security personnel with role-based permissions granted from senior management to access the data as well as senior managers based on a need to know. |
| **MONITORING** | |
| **17. Will this information system provide the capability to identify, locate, and monitor individuals?** | Yes, this is a security system specifically designed to authentic users as they interact with ingress points. The data provides the capability to identify individuals and log current and prior area access. This is a point in time capture, but the collection of system log files can be used to determine when an individual entered the facility and possibly a user's schedule. |
| **18. What kinds of information are collected as a function of the monitoring of individuals?** | Name, BNL Life Number, Department, and Facility Access. |
| **19. Are controls implemented to prevent unauthorized monitoring of individuals?** | Yes. Access to and use of data which may assist in the monitoring of individuals is protected by a series of controls including role and permission-based monitoring controls and periodic auditing. The Laboratory Protection Division actively ensures the accuracy and currency of PII in the system via auditing as outlined in ID Badging Procedure (PS-2). In addition, system protections take into account NIST SP 800-53 guidelines to minimize privacy impacts. |
| **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.** | The Laboratory Protection Division actively ensures the accuracy and currency of PII in the system via auditing as outlined in ID Badging Procedure (PS-2). |
| **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. Information system is not operated in any other sites. |
| **RECORDS MANAGEMENT** | |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **22. Identify the record(s).** | BNL ADM 1000-1717 Key Accountability files for High Security Areas<br><br>Files relating to the accountability of keys issued which include an active inventory of keys along with dates issued, life & key numbers. These keys are for limited and higher security areas, or for the protection of classified/special nuclear materials. |
| **23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.** | ADM-18.16a – DM-18.16A0 |
| **24. Records Contact** | Lauren Heller<br><br>(631) 344-7692<br><br>lheller@bnl.gov |
| **ACCESS, SAFEGUARDS & SECURITY** | |
| **25. What controls are in place to protect the data from unauthorized access, modification or use?** | CCure is configured and controlled based on the NIST SP 800-53 moderate level system control requirements. Access to and use of data which may assist in the monitoring of individuals is protected by a series of controls including role and permission-based monitoring controls and periodic auditing. Access to data is based strictly on a need to know. The Laboratory Protection Division actively ensures the accuracy and currency of PII in the system via auditing as outlined in ID Badging Procedure (PS-2). |
| **26. Who will have access to PII data?** | Authorized databased and system administrators, security personnel with role-based permissions, and authorized senior management may have access to the data. |
| **27. How is access to PII data determined?** | Role-based permissions are granted from senior management to access the data based on a need to know. Personnel will not have access to PII with a specified business purpose. |
| **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?** | Senior management and other authorized managers grant role-based permissions to access the data. |
| **END OF MODULE II** | |

# SIGNATURE PAGE

| | Signature | Date |
|---|---|---|
| **System Owner** | Virgilio Martinez<br>Digitally signed by Virgilio Martinez<br>Date: 2022.09.20 13:58:59 -04'00'<br><br>ROBERT GORDON<br>Digitally signed by ROBERT GORDON<br>Date: 2022.09.20 17:45:06 -04'00' | |
| **Local Privacy Act Officer** | Miriam Bartos<br>Digitally signed by Miriam Bartos<br>Date: 2022.08.31 09:39:09 -05'00' | |
| ***Ken Hunt***<br>**Chief Privacy Officer** | William K. Hunt<br>Digitally signed by William K. Hunt<br>Date: 2022.08.31 10:28:38 -04'00' | |