Privacy Impact Assessment (PIA): CDC - ESS - QTR2 - 2025 - CDC8720421

Created Date: 5/29/2025 4:01 PM Last Updated: 6/24/2025 8:01 PM

## Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

## Instructions

Review the following steps to complete this questionnaire:

**1) Answer questions.** Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

**2) Add Comments.** You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

**3) Change the Status.** You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

**4) Save/Exit the Questionnaire.** You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

## General Information

| | | | |
|---|---|---|---|
| **PIA Name:** | CDC - ESS - QTR2 - 2025 - CDC8720421 | **PIA ID:** | 3244097 |
| **Name of Component:** | CDC - Electronic Security Systems | **Name of ATO Boundary:** | Electronic Security Systems |
| **Overall Status:** |  | **PIA Queue:** | |
| **Submitter:** | | **# Days Open:** | 34 |
| **Submission Status:** | Re-Submitted | **Submit Date:** | 6/11/2025 |
| **Next Assessment Date:** | N/A | **Expiration Date:** | 6/23/2028 |
| **Office:** | | **OPDIV:** | CDC |
| **Security Categorization:** | High | **OpDiv PIA ID:** | CDC8720421 |
| **Legacy PIA ID:** | | **Make PIA available to Public?:** | Yes |

| | | |
|---|---|---|
| **1:** | Identify the Enterprise Performance Lifecycle Phase of the system. | Operations and Maintenance |
| **2:** | Is this a FISMA-Reportable system? | Yes |
| **3:** | Does the system have or is it covered by a Security Authorization to Operate (ATO)? | Yes |
| **4:** | ATO Date or Planned ATO Date. | 6/17/2022 |
| **5:** | Is the system or electronic information collection, agency or contractor operated? | Agency |

## PTA

### PTA

| | | |
|---|---|---|
| **PTA - 2:** | Indicate the following reason(s) for this PTA. Choose from the following options. | PIA Validation (PIA Refresh) |

| | | |
|---|---|---|
| **PTA - 2A:** | Describe in further detail any changes to the system that have occurred since the last PIA. | The only approved changes made by the Business Steward/Owner since the last review are listed below:<br><br>--System Name: The previous name of this system/component was Intrusion Detection Assessment System (IDAS) which is now called Electronic Security System (ESS) which is now reflected in the Enterprise System Catalog (ESC)<br><br>--The impact level elevated to High - Information associated with security management at the Centers for Disease Control and Prevention (CDC) buildings that house high-containment laboratories (HCL). Included are alarms and alert communications and interconnections for security management systems and automated control systems that support security management processes.<br><br>--The removal of the following collected information (email, employment status, text) which are no longer data elements used within the ESS environment. |
| **PTA - 3:** | Is the data contained in the system owned by the agency or contractor? | Agency |
| **PTA - 4:** | Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions. | The Electronic Security Systems (ESS) is an integrated system comprised of an existing Internet Protocol (IP) Based Video Surveillance System (IP Surveillance) digital network video recorder system (NVRS) with integral video motion detection (VMD) function, and a physical access control system (PACS).<br><br>The ESS purpose of the system, functions to control physical access and to organize and present video and event information to security operators to assist them in assessing and disposition of potential threats to CDC Select Agent (SA) which is a high-containment laboratory (HCL) and repositories. PACS is installed in Atlanta, Morgantown, Fort Collins, San Juan, Hyattsville, Research Triangle Park (RTP), Anchorage, Spokane, Pittsburg and Cincinnati. IP Surveillance and NVR systems are integrated with the PACS in Atlanta, Fort Collins, San Juan, Morgantown, Spokane, Cincinnati, RTP, Hyattsville, and Anchorage. |

| | | |
|---|---|---|
| **PTA - 5:** | List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored. | ESS utilizes “name” and “photographic” data elements to identify, match and manage individuals within the Physical Access Control System (PACS) to provide and monitor controlled access to restricted areas within the secure perimeters of CDC owned and leased facilities. “Name” and “photographic” data elements are present on Physical Identification Verification (PIV) in accordance with Homeland Security Presidential Directive -12 and NIST 201-3. “Biometrics” are again used within the PACS to manage access to controlled spaces where PIV are not applicable due to Personal Protective Equipment (PPE) requirements with a particular space, typically lab environments. ESS video data elements is a Code of Federal Regulations (CFR) title 42.71.11 compliance requirement supporting the Federal Select Agent Program. "Event information" to security operators to assist them in assessing and disposition of potential threats |
| **PTA - 5A:** | Are user credentials used to access the system? | |
| **PTA - 5B:** | Please identify the type of user credentials used to access the system. | HHS User Credentials<br>HHS/OpDiv PIV Card<br>HHS Email Address<br>HHS Username<br>Password |
| **PTA - 6:** | Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual. | ESS utilizes “name” and “photographic” data elements to identify, match and manage individuals within the Physical Access Control System (PACS) to provide and monitor controlled access to restricted areas within the secure perimeters of CDC owned and leased facilities. “Name” and “photographic” data elements are present on Physical Identification Verification (PIV) in accordance with Homeland Security Presidential Directive -12 and NIST 201-3. “Biometrics” are again used within the PACS to manage access to controlled spaces where PIV are not applicable due to Personal Protective Equipment (PPE) requirements with a particular space, typically lab environments. ESS video data elements is a Code of Federal Regulations (CFR) title 42.71.11 compliance requirement supporting the Federal Select Agent Program. ESS shares event information with security operators to assist them in assessing and disposition of potential threats |
| **PTA - 7:** | Does the system collect, maintain, use or share PII? | Yes |
| **PTA - 7A:** | Does this include Sensitive PII as defined by HHS? | Yes |
| **PTA - 8:** | Does the system include a website or online application? | No |
| **PTA - 8A:** | Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)? | |
| **PTA - 9:** | Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response. | |
| **PTA - 10:** | Does the website have a posted privacy notice? | |

| | | |
|---|---|---|
| **PTA - 11:** | Does the website contain links to non-federal government websites external to HHS? | |
| **PTA - 11A:** | Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS? | |
| **PTA - 12:** | Does the website use web measurement and customization technology? | |
| **PTA - 12A:** | Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII. | |
| **PTA - 13:** | Does the website have any information or pages directed at children under the age of thirteen? | |
| **PTA - 13A:** | Does the website collect PII from children under the age thirteen? | |
| **PTA - 13B:** | Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected? | |
| **PTA - 14:** | Does the system have a mobile application? | No |
| **PTA - 14A:** | Is the mobile application HHS developed and managed or a third-party application? | |
| **PTA - 15:** | Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response. | |
| **PTA - 16:** | Does the mobile application/ have a privacy notice? | |
| **PTA - 17:** | Does the mobile application contain links to non-federal government websites external to HHS? | |
| **PTA - 17A:** | Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS? | |
| **PTA - 18:** | Does the mobile application use measurement and customization technology? | |
| **PTA - 18A:** | Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected. | |
| **PTA - 19:** | Does the mobile application have any information or pages directed at children under the age of thirteen? | |
| **PTA - 19A:** | Does the mobile application collect PII from children under the age thirteen? | |
| **PTA - 19B:** | Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected? | |
| **PTA - 20:** | Is there a third-party website or application (TPWA) associated with the system? | No |
| **PTA - 21:** | Does this system use artificial intelligence (AI) tools or technologies? | No |

## PIA

### PIA

| | | |
|---|---|---|
| **PIA - 1:** | Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share. | Name<br>Photographic Identifiers<br>Biometric Identifiers<br>Other - Free text Field - Video |
| **PIA - 2:** | Indicate the categories of individuals about whom PII is collected, maintained or shared. | Employees/ HHS Direct Contractors<br>Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors) |

| | | |
|---|---|---|
| **PIA - 3:** | Indicate the approximate number of individuals whose PII is maintained in the system. | Above 2000 |
| **PIA - 4:** | For what primary purpose is the PII used? | Personally Identifiable Information (PII) is used to establish the identity of an individual seeking to gain access to a Centers for Disease Control (CDC) facility or asset. |
| **PIA - 5:** | Describe any secondary uses for which the PII will be used (e.g. testing, training or research). | The secondary uses for which the PII will be used is (1) to ensure the safety and security of Health and Human Services (HHS) facilities, systems, or information, and our occupants and users; (2) to verify that all persons entering federal facilities, using federal information resources, or accessing classified information are authorized to do so. |
| **PIA - 6:** | Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. | N/A<br><br>SSN and/or Taxpayer ID are not collected. |
| **PIA - 6A:** | Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. | N/A<br><br>SSN are not collected. |
| **PIA - 7:** | Identify legal authorities governing information use and disclosure specific to the system and program. | 5 U.S.C. 301; Information Technology Management Reform Act of 1996 (Pub. L. 104-106, sec. 5113); Federal Property and Administrative Act of 1949, as amended. |
| **PIA - 8:** | Are records in the system retrieved by one or more PII data elements? | No |
| **PIA - 8A:** | Please specify which PII data elements are used to retrieve records. | |
| **PIA - 8B:** | Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development. | 09-90-0777 "Facility and Resource Access Control Records |
| **PIA - 9:** | Identify the sources of PII in the system. | Government Sources<br><br>Within the OPDIV |
| **PIA - 10:** | Is there an Office of Management and Budget (OMB) information collection approval number? | No |
| **PIA - 10A:** | Provide the information collection approval number. | |
| **PIA - 10B:** | Identify the OMB information collection approval number expiration date. | |
| **PIA - 10C:** | Explain why an OMB information collection approval number is not required. | Users are required to provide their PII prior to gaining access to the Electronic Security System (ESS); it is required to set up an account. |
| **PIA - 11:** | Is the PII shared with other organizations outside the system's Operating Division? | No |
| **PIA - 11A:** | Identify with whom the PII is shared or disclosed. | |
| **PIA - 11B:** | Please provide the purpose(s) for the disclosures described in PIA - 11A. | |
| **PIA - 11C:** | List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)). | |
| **PIA - 11D:** | Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not. | |

| | | |
|---|---|---|
| **PIA - 12:** | Is the submission of PII by individuals voluntary or mandatory? | Voluntary |
| **PIA - 12A:** | If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties. | |
| **PIA - 13:** | Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason. | PII is collected during the investigation process which is a federal government job requirement. Those who refuse to provide personal information will not meet the requirements of the job and will therefore not be considered further. Current employees who do not meet these requirements will be terminated. |
| **PIA - 14:** | Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained. | The identification of individuals complies with Homeland Security Presidential Directive 12 (HSPD-12) for the collection of Personally Identifiable Information (PII). Currently, there is no established process to notify individuals of any changes to applications, as the primary purpose of data collection is to fulfill federal government compliance and mandates. The PII provided by individuals remains consistent and does not change over time. Furthermore, all visitors are required to present valid identification during each visit, in accordance with HSPD-12, the Interagency Security Committee (ISC), and the Real Identification (ID) Act. There is no secondary use of the collected PII, which eliminates the need for any modifications or alterations to that information |
| **PIA - 15:** | Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not. | In the event that individuals feel their PII was obtained inappropriately, they should email the point of contact for this issue: Office of Safety, Security, and Asset Management (OSSAM) Chief - ossam@cdc.gov, PERSONNEL SECURITY & ADJUDICATION (ADJ) at cdcsecurit@cdc.gov. Once the Point of Contact is notified the request is reviewed and the proper modifications are made and communicated back to the originating party. |
| **PIA - 16:** | Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not. | The ESS account auditing process entails review of user accounts annually by OSSAM Information Technology (IT) Security support and annually review of policies governing auditing by the Security Steward, Business Steward and Technical Steward. The policy must be signed by the Business Steward, Security Steward and Deputy Director of OSSAM annually. Access to the system is managed through active directory (AD); and users are removed from the system when they are removed from AD. AD is a separate system covered by a separate PIA. For users whose roles change due to job reassignment of retirement, OSSAM support staff relies on communication via phone or email to notify that the account needs to be modified. |
| **PIA - 17:** | Identify who will have access to the PII in the system. | Users<br>Administrators |
| **PIA - 17A:** | Select the type of contractor. | |

| | | |
|---|---|---|
| **PIA - 17B:** | Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices? | |
| **PIA - 18:** | Provide the reason why each of the groups identified in PIA - 17 needs access to PII. | Users:<br><br>Data entry, Life Cycle Management, and assignment of access rights.<br><br>Administrators:<br><br>Enterprise Data entry, Life Cycle Management, assignment of access rights, backup and restore capabilities. |
| **PIA - 19:** | Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. | The system makes extensive use of roles and access privileges to enforce access to PII. System users are approved via business case and access is managed by the Active Directory (AD) group membership. |
| **PIA - 20:** | Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job. | The least privilege model is used to ensure that those having access to the PII in the system only access the minimum amount necessary to perform their job. ESS relies on Active Directory which further enforces the most restrictive access level rights needed by system users for the performance of their tasks. |
| **PIA - 21:** | Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained. | Security and Privacy Awareness Training (SAT), and HHS Annual Ethics Training (AET) is an annual requirement for CDC Agency for Toxic Substances and Disease Registry (ATSDR) employees. This is mandated for all CDC Full-Time Equivalent (FTE), Fellows and Locally Employed.<br><br>Also, Senior Leaders are required to take Role-Based Training (RBT). This training (RBT) is designed to ensure protection of CDC information systems and data and meet HHS and federal policy, all personnel with Significant Security Responsibilities (SSR) are required to complete mandatory HHS role based training. This training provides personnel with SSR the necessary guidelines and continued education to reduce risks to CDC data and information systems. |
| **PIA - 22:** | Describe the training system users receive (above and beyond general security and privacy awareness training). | System users undergo annual Role Based Training. This training provides guidance base on there role and responsibility due to handling of data concerning its integrity, availability and confidentiality. In addition, users must be verified by OSSAM process and sign the ESS Rules of Behavior. |

| | | |
|---|---|---|
| **PIA - 23:** | Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s). | Johnson Controls (P2000) physical access control system and Health and Human Services Identity Management System (HHS-IDMS): Paper and electronic Personal Identity Verification (PIV) Credential requests and Physical Access Control System (PACS) authorization records are maintained for the period of the badge holders service and for at least five years afterwards before being archived.<br><br>Electronic feed(s) from other electronic systems and transaction histories from terminal controllers - Dispose when no longer needed (Governance, Risk, and Compliance (GRC) 4.3 item 020)<br><br>Non-electronic records manually data entered - 5 years (General Records Schedule (GRS) 4.3 item - whichever is applicable >010, 011, 012<) |
| **PIA - 24:** | Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response. | Administrative controls: In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and the HHS Information Systems Security and Privacy Policy, CDC/OSSAM requires annual information security and privacy awareness for all agency personnel and contractors who access information systems that support the operation and assets of the agency. Training is continuously assessed to review efficiency and refreshed annually based on emerging trends. CDC will safeguard the privacy of individuals to the fullest extent possible, while at the same time permit disclosure of records necessary to fulfill the mission of CDC. CDC will also maintain and readily provide information to individuals who seek notification of disclosures and access to their own records contained in systems of records to the extent allowable under the Privacy Act.<br><br>Technical controls: ESS uses smart cards, passwords and firewalls to manage access to resources and systems and provide protection for those resources, systems and data. Access to computerized records is limited, through use of user identifications (IDs) and password entry.<br><br>Physical controls: Access to data is protected by the use of card readers, locked doors, security guards, and video cameras. Paper records are stored in locked cabinets or in secured rooms with access limited to those personnel whose official duties require access. If data is removed from the system, it is marked appropriately and handled in accordance with the data categorization. |

## Review & Comments

### Privacy Analyst Review

| | | | |
|---|---|---|---|
| **OpDiv Privacy Analyst Review Status:** | Approved | **Privacy Analyst Review Date:** | 6/11/2025 |
| **Privacy Analyst Comments:** | | **Privacy Analyst Days Open:** | |

### SOP Review

| | | | |
|---|---|---|---|
| **SOP Review Status:** | Approved | **SOP Signature:** | |
| **SOP Comments:** | Approved on behalf of Beverly Walker. | **SOP Review Date:** | 6/11/2025 |
| | | **SOP Days Open:** | 0 |

### Agency Privacy Analyst Review

| | | | |
|---|---|---|---|
| **Agency Privacy Analyst Review Status:** | Approved | **Agency Privacy Analyst Review Date:** | 6/13/2025 |
| **Agency Privacy Analyst Review Comments:** | Reviewer: Shanai Shobowale<br><br>6/13/2025 This PIA is ready for SAOP review and approval. | **Agency Privacy Analyst Days Open:** | 2 |

### SAOP Review

| | | | |
|---|---|---|---|
| **SAOP Review Status:** | Approved | **SAOP Signature:** | Archer Signature_Bridget Guenther.docx |
| **SAOP Comments:** | | **SAOP Review Date:** | 6/24/2025 |
| | | **SAOP Days Open:** | 11 |

### Supporting Document(s)

| Name | Size | Type | Upload Date | Downloads |
|---|---|---|---|---|
| No Records Found | | | | |

## Comments

| Question Name | Submitter | Date | Comment | Attachment |
|---|---|---|---|---|
| PIA - 1 | Data Feed Service, piafrmcdc | 5/29/2025 | In accordance with the current PTA, “The removal of the following collected information (email, employment status, text) which are no longer data elements used within the ESS environment.” Please remove or confirm the email address and employment status as a type of PII that is collected, maintained, or shared. | |
| PIA - 1 | Data Feed Service, piafrmcdc | 5/29/2025 | In accordance with the current PTA, “ESS video” is collected, maintained, or shared which may contain PII. Please add this as a type of PII. | |
| PIA - 10C | Data Feed Service, piafrmcdc | 5/29/2025 | First use, please spell out the acronyms for “ESS”. | |
| PIA - 14 | Data Feed Service, piafrmcdc | 5/29/2025 | In accordance with the current PTA, “The removal of the following collected information (email, employment status, text) which are no longer data elements used within the ESS environment.” Please remove or confirm that the email address is being utilized. | |
| PIA - 21 | Data Feed Service, piafrmcdc | 5/29/2025 | First use, please spell out the acronyms for “CDC/ATSDR” and “FTEs”. | |
| PIA - 15 | Data Feed Service, piafrmcdc | 6/10/2025 | Just to confirm, there is a closing parenthesis but no opening parenthesis. Is any information missing in this sentence or email address? | |
| PIA - 23 | Data Feed Service, piafrmcdc | 6/10/2025 | Define all acronyms upon first use. | |
| PIA - 1 | BLAND, CRYSTAL | 6/13/2025 | On the next iteration of the PTA:<br><br>PTA-5: please include "Biometric identifiers" as one of the PII elements collected. | |

## Admin Section

| | | | |
|---|---|---|---|
| **Is OpDiv Privacy Analyst Approved ?:** | 1 | **Is OpDiv Privacy Analyst Return ? :** | 0 |
| | | **Is SOP Return ?:** | 0 |
| **Is Agency Privacy Analyst Approve ?:** | 1 | **Is Agency Privacy Analyst Return ?:** | 0 |
| **Is SAOP Approved?:** | 1 | **Is SAOP Return ?:** | 0 |
| **Total Approved:** | 4 | **Total Return:** | 0 |
| **Total Approval Required:** | 4 | | |

## Miscellaneous Fields

| | | | |
|---|---|---|---|
| **Last Updated:** | 6/24/2025 8:01 PM | **History Log:** | View History Log |