Privacy Impact Assessment
for the

U.S. Secret Service
Credential Distribution System

DHS/USSS/PIA-012

July 11, 2013

Contact Point
Latita Payne
Privacy Officer
United States Secret Service
(202) 406-5838

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (USSS) Information Resources Management Division has created the Credentialing Distribution System (CreDS). CreDS provides the USSS with the capability to electronically collect National Special Security Event (NSSE) prospective event worker information, enable automated criminal background checks, and produce appropriate event credentials. The USSS is conducting this Privacy Impact Assessment (PIA) because CreDS handles personally identifiable information (PII) regarding NSSE workers and applicants.

Overview

The Dignitary Protective Division (DPD) within the USSS is tasked with coordinating physical security for NSSEs. DPD prevents terrorist and criminal attacks on NSSEs and their participants, which often include USSS protectees. DPD collects PII in order to assess the criminal history of non-USSS prospective event workers and make a security determination regarding whether to grant or deny them access to the NSSE. Examples of event workers are the media, caterers, law enforcement, and any other organizational officials that are not employed by the USSS.

The credentialing process begins with a public facing website that allows for the secure, controlled entry of specific PII by prospective event workers (also referred to as applicants) or designated Points of Contact (POC). The POC serves as the coordinator for specific groups of applicants. The POC may either directly enter the worker's required information, or may create a basic account for that worker to enter his or her own data directly into the CreDS website. CreDS includes internal and external firewalls and Federal Information Processing Standards (FIPS) 140-2 validated encryption for data at rest.

CreDS then conducts security name checks on submitted applicants. These name checks are performed through the National Crime Information Center (NCIC) information system and other law enforcement databases. Law enforcement officials' information is entered into the CreDS database for credentialing, but they are not name checked.

Once the security name check is completed, and if the applicant is granted access to the event, CreDS produces a physical credential for the applicant. The card may be presented to a CreDS card reading device to indicate to USSS personnel whether entry is to be allowed.

Overall privacy risks associated with CreDS are related to the accuracy of individual data input into CreDS, unauthorized access and inappropriate dissemination of CreDS data, longevity of CreDS data retention, external sharing of CreDS data, and risks associated with individual access to stored CreDS information. Mitigation strategies have been put in place to address all of the identified privacy risks as outlined below.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The collection of information in support of CreDS is authorized by the following legal authorities: 18 U.S.C. §§ 3056 and 3056A; Powers, Authorities, and Duties of United States Secret Service.

1.2 What Privacy Act System of Records Notice(s) (SORN) apply to the information?

CreDS is covered by DHS/USSS-004 Protection Information System SORN, 76 Fed. Reg. 66940 (October 28, 2011).[1]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. Security Authorization (SA) was completed on March 22, 2012, with the granting of an Authority to Operate (ATO). A System Security Plan was submitted for evaluation and a certification team evaluated all CreDS security controls before submitting a Security Assessment Report (SAR) to the Authorizing Official (AO).

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. The Secret Service is covering these materials under General Records Schedule (GRS) 18, item 17 ("Visitor Control Files"); GRS 18, item 22a and 22c ("Case files documenting the processing of investigations on […] other persons, such as those performing work for a Federal agency under contract, who require an approval before having access to Government [controlled] facilities"; and GRS 11, Item 4 ("Identification credentials and related papers").

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No, as a law enforcement investigative instrument, it is exempt under the provisions of 44 U.S.C. § 3518(c) and 18 U.S.C. § 3056(b).

[1] http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

All non-USSS event workers must undergo an appropriate background check before being admitted to or allowed to enter a NSSE. The following information from these event workers is required to be entered into CreDS in order to conduct appropriate background checks and allow DPD to print credentials:

- Full name
- Date of Birth
- Gender
- Country of birth
- Email address (for POC only)
- Social Security number (SSN) or Passport Number and Country
- City and state of residence/visit location
- Organization name
- Job function
- Weapon carrier status (for Law Enforcement only)
- Photograph

Other PII that may be recorded in CreDS includes the following:

- Workers/Applicants and/or POC
  - Drivers license number
  - FBI number
  - State criminal ID number
  - Alien identification number
  - Other identifying number
  - Arrest record

2.2 What are the sources of the information and how is the information collected for the project?

Information is gathered by CreDS directly from a designated POC or directly from applicants. Individual NSSE applicants input and upload their personal information and photographs to the CreDS public facing website.

Additional information regarding specific personal records is obtained from NCIC and other law enforcement databases.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, none of the data comes from publicly available or commercial sources.

2.4 Discuss how accuracy of the data is ensured.

CreDS has assigned an Event POC. The registered individuals are responsible for initially ensuring the accuracy of the information prior to submitting it to DPD for processing.

Information submitted into CreDS is checked for consistency between the applicant's full name, date of birth, and either SSN or Passport Number. A request cannot be resolved until these pieces of data are consistent with one another. USSS may try to resolve minor issues such as inconsistent name spellings, but generally an inconsistent request will be returned to the requesting account POC for clarification.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Because CreDS is designed to collect PII directly from the applicants concerned, there is a risk that the applicant may not enter complete and valid data in an attempt to avoid being linked to their criminal history.

Mitigation: CreDS will not accept incomplete results and will ensure that applicants or a POC have entered complete information prior to presenting the information to CreDS personnel for evaluation. Trained DPD personnel assess the reported information against government databases to ensure its consistency. If data is discovered to be erroneous or invalid, these trained DPD personnel address the inconsistency issue directly with the applicant or the applicant's designated POC.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The information gathered by CreDS is used to support the USSS in accomplishing its protective mission. CreDS assists DPD in managing and vetting individuals, then creating and distributing NSSE credentials to effectively control and manage access to specific special events. The information gathered, including SSN, assists the USSS in identifying individual threats or potential threats to the safety of individuals, events, and facilities protected by the USSS by denying access to the event by unauthorized individuals. In addition, the information is used to produce the physical credential which includes, for example, the individual's name and photograph.

DPD officers, agents, and Administrative, Professional, and Technical (APT) personnel use the information gathered from CreDS to make a risk assessment of the applicant based on multiple factors, for example, types and severity of law enforcement encounters, length of time since any such encounters, and the applicant's intended role at the NSSE.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

CreDS does not use technology to discover or locate predictive patterns or anomalies. CreDS uses current USSS electronic searches, queries, or analyses in law enforcement databases in order to determine whether or not an individual is cleared and/or authorized to receive an NSSE access credential. The electronic searches use existing query rules as established for the relevant law enforcement databases. These rules are not changed by the USSS and are controlled by the governing bodies that own the law enforcement databases.

3.3 Are there other components with assigned roles and responsibilities within the system?

While CreDS utilizes the information gathered from various law enforcement databases, there are no other DHS components with assigned roles and responsibilities within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information.

Privacy Risk: There is a privacy risk of unauthorized access to information maintained by CreDS.

Mitigation: The USSS has mitigated this risk by implementing strong security controls for CreDS. These include user accountability and validity of identification, user audit logs for significant activity, system time-out after twenty minutes of inactivity, Role Based Access Control (RBAC) limited to authorized individuals with a verifiable need-to-know, web site account lockout after three unsuccessful attempts, and a security warning to users that unauthorized, improper use or access to the system may result in disciplinary action, as well as civil and criminal penalties.

Privacy Risk: There is a privacy risk of inappropriate dissemination of information maintained by CreDS.

Mitigation: All DPD personnel complete annual agency mandated privacy and security training, which stresses the importance of appropriate and authorized use of PII in government systems.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

This PIA provides notice to the general public on the collection and use of PII. An assigned POC is informed of the information necessary to be collected and how it will be used. It is expected that the POC will provide this information to applicants.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All information provided is voluntary, though refusal to provide information may negatively affect the background check and approval process.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware of the manner in which CreDS uses the data it collects.

Mitigation: This PIA and the USSS Protection Information SORN serve as public notice of the existence of CreDS and the manner in which CreDS uses, maintains, and safeguards PII. The information is used only for the purpose for which it was provided through the public notice of this PIA. Event coordinators inform the applicants of the necessary information to be collected and how it will be used.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Consistent with the authorities cited in section 1.4, any Visitor Control Files will be retained for 2 years. Any corresponding investigative case files will be retained for 5 years. Returned identification credentials and related papers will be destroyed after three months.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information in CreDS may be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The information in CreDS is retained for the timeframes outlined in Question 5.1 to allow the USSS to manage, vet, create, and distribute NSSE credentials to effectively control and manage access to specific special events while identifying potential threats to the safety of individuals, events, and facilities protected by the USSS. After that time, information is then deleted from the system. The retention period is appropriate given the USSS protective mission and the importance of the law enforcement data to accomplish this mission.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

As outlined in Section 2.1, CreDS routinely submits applicant information to law enforcement databases such as NCIC in order to receive security relevant information and complete background checks.

CreDS does not as a matter of routine, or in any automated way, share these results outside of its purpose of validating event workers. If there were an event of criminal investigative or protective interest, USSS personnel might manually share data contained in CreDS with federal, state, or local law enforcement agencies that have a need to know.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Any information maintained in CreDS may be shared in accordance with the purposes and routine uses specified in the DHS/USSS-004 Protection Information System SORN, 76 Fed. Reg. 66940 (October 28, 2011), in support of the USSS protective mission.

6.3 Does the project place limitations on re-dissemination?

Yes, the information is shared only upon verification of need-to-know and in conjunction with adequate warnings regarding improper re-dissemination. USSS generally provides adequate warnings regarding improper re-dissemination. External law enforcement agencies may have requirements on further dissemination of the information gathered through CreDS.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

CreDS maintains application level audit logs, which record transactions sent and received from external agencies and departments. These audit logs are archived in accordance with NARA file retention guidelines.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The privacy risk associated with this external sharing is unauthorized access or disclosure of the information maintained in CreDS.

Mitigation: The sharing of information described above is in accordance with appropriate routine uses and legally mandated sharing. This information is shared only upon verification of need-to-know and in conjunction with adequate warnings regarding improper re-dissemination.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

As a protection information system owned by the USSS, DHS/USSS-004 Protection Information System SORN, 76 Fed. Reg. 66940 (October 28, 2011), permits CreDS to be excluded from the access and redress provisions of the Privacy Act in order to prevent harm to law enforcement investigations or interests. However, access requests are considered on a case-by-case basis if made in writing to the USSS Freedom of Information Act (FOIA)/Privacy Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-54, Washington, D.C. 20223, as specified in the Protection Information System SORN.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The CreDS website will detect some erroneously entered input automatically and prompt an individual to re-enter the data. Once submitted, at a minimum the Full Name, Date of Birth, and either SSN or Passport Number and Country must all be consistent. Inconsistent entries may be investigated by agents or clarified with the assigned POC to try and resolve the inconsistency.

If an application is declined, the DPD Assistant to the Special Agent in Charge (ATSAIC) for CreDS will notify the POC for that applicant. If the applicant wishes to appeal, this appeal would first be routed through the ATSAIC and may be reconsidered by the DPD Special Agent in Charge.

CreDS relies on information from external law enforcement databases. Since CreDS is a consumer and not a provider of information to these systems, correcting erroneous information in these databases exceeds the scope of CreDS' ability.

7.3 How does the project notify individuals about the procedures for correcting their information?

The mechanism for requesting correction of information is specified in the DHS/USSS-004 Protection Information System SORN, 76 Fed. Reg. 66940 (October 28, 2011), and in this PIA. In the event of a negative finding, the DPD ATSAIC would notify the assigned POC, who would notify the applicant and provide appeal information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that an applicant may have limited access or ability to correct their information.

Mitigation: The CreDS application entry interface is available approximately 6 weeks prior to an event and up through 72 hours prior to the event. CreDS personnel require 72 hours to validate applicants. Individuals that apply late in the process may not have time to complete an appeal prior to the event. Appeals have been and are expected to be an infrequent and exceptional occurrence. Senior DPD personnel will make every effort to resolve these ahead of the event.

Applicants may also request access to information about them under the FOIA and Privacy Act and may also request that their information be corrected. As a protection information system owned by

the USSS, DHS/USSS-004 Protection Information System SORN, 76 Fed. Reg. 66940 (October 28, 2011), permits CreDS to be excluded from the access and redress provisions of the Privacy Act in order to prevent harm to law enforcement investigations or interests.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

All USSS information systems are audited regularly to ensure appropriate use of and access to information. CreDS supports routine audit logging and monitoring and unusual user activity is investigated.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All USSS employees are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. DHS has published the "Handbook for Safeguarding Sensitive PII," providing employees and contractors additional guidance.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

A POC is chosen by the entities whose personnel or affiliates are seeking a credential. For example, multiple POCs may be identified to facilitate credentials for members of the media, local law enforcement, and Fire\Life\Safety personnel. Individual applicants may only access their own information. A POC may only access information related to his or her own applicants.

DHS physical and information security policies dictate who may access USSS computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to USSS computers. Access to the information is strictly limited by access controls to those who require it for completion of their official duties.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

CreDS is a USSS-only system and uses previously existing agreements to share information between external law enforcement entities. It is not anticipated that CreDS will be used by other DHS components or external entities.

Responsible Officials

Victor Erevia
Assistant Director – Protective Operations
U.S. Secret Service

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security