Privacy Impact Assessment Update
for the

U.S. Secret Service
Electronic Name Check System (E-Check)

DHS/USSS/PIA-012(a)

July 23, 2015

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

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service (USSS) Information Resources Management Division has established a system called Credentialing Distribution System (CreDS). CreDS provides the USSS with the capability to electronically collect National Special Security Event (NSSE) prospective event worker information to enable automated criminal background checks. The Privacy Impact Assessment (PIA) for CreDS was published in July 2013. This PIA Update is being completed because CreDS is being renamed to the Electronic Name Check System (E-Check).

Overview

The USSS is tasked by statute[1] with coordinating physical security for NSSEs. The USSS Dignitary Protective Division (DPD) prevents and counters terrorist and criminal attacks on NSSEs and their participants, who often include USSS protectees. DPD collects personally identifiable information (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 USSS.

The credentialing process begins with a public facing website, which allows for the secure, controlled entry of specific PII by prospective event workers (also referred to as applicants) or a designated Point of Contact (POC). These POCs serve 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 E-Check website. E-Check includes internal and external firewalls and Federal Information Processing Standards (FIPS) 140-2 validated encryption for data at rest.

E-Check then conducts security name checks on submitted applicants. These name checks are performed through the National Crime Information Center (NCIC)[2] information system, a nationwide information system established by the Federal Bureau of Investigation (FBI) as a service to criminal justice agencies and other law enforcement databases. Law enforcement officials' information is entered into the E-Check 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, E-Check produces a physical credential for the applicant. The card may be presented to a

[1] 18 U.S.C. § 3056(e), "Powers, authorities, and duties of the United States Secret Service."
[2] *See* http://www.fbi.gov/about-us/cjis/ncic for more information about NCIC.

E-Check card reading device to indicate to USSS personnel whether to allow entry. Overall privacy risks associated with E-Check are related to the accuracy of individual data input into E-Check, unauthorized access and inappropriate dissemination of E-Check data, longevity of E-Check data retention, external sharing of E-Check data, and risks associated with individual access to stored E-Check information. USSS has developed mitigation strategies to address all of the identified privacy risks as outlined below.

Reason for the PIA Update

This PIA is being updated to reflect the system name change from USSS Credentialing Distribution System (CreDS) to Electronic Name Check System.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

There is no change in the specific legal authorities and/or agreements that permit and define the collection of information in E-Check.

Characterization of the Information

There is no change in the type of information collected in E-Check. The following information from event workers will continue to be entered into E-Check in order to conduct appropriate background checks:

- Full name;
- Date of birth;
- Gender;
- Country of birth;
- Email address (for POCs 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); and
- Photograph.

Other PII that may be recorded in E-Check (following the background check) includes Workers/Applicants and/or POCs:

- Driver's license number
- FBI number
- State criminal ID number
- Alien identification number
- Other identifying number
- Arrest record

Information submitted into E-Check will be 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.

Uses of the Information

There are no changes in the uses of the information.

Data Retention by the project

The retention period for E-Check has not changed.

Information Sharing

The internal or external sharing and disclosure have not changed with this update.

Redress

Access, redress, and correction rights have not changed with this update.

Auditing and Accountability

The system will continue to take all necessary measures to ensure that the information stored within E-Check is used in accordance with the stated practices in this PIA Update. All USSS information systems are audited regularly to ensure appropriate use of and access to information. E-Check supports routine audit logging and monitoring and unusual user activity is investigated.

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.

POCs are 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 who have created their own log-on accounts may access their own information. POCs may only access information related to their 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.

E-Check is a USSS-only system and uses previously existing agreements to share information between external law enforcement entities. It is not anticipated that E-Check will be utilized by other DHS components or external entities. Such a change would trigger an update to this PIA.

Responsible Official

Latita Payne
Privacy Officer
United States Secret Service
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security