Privacy Impact Assessment Update
for the

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

DHS/USSS/PIA-012(b)

September 28, 2016

Contact Point
Steve Sepulveda
Special Agent In Charge
Information Resources Management Division
Chief Information Office
United States Secret Service
(202) 406-5729

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 established a system called Electronic Name Check System (E-Check). E-Check provides USSS with the capability to electronically collect prospective event participant information to enable automated criminal background checks. This PIA Update is being completed to reflect changes associated with USSS credentialing in conjunction with large events, to include National Special Security Events (NSSE), which have been partially outsourced to a third-party vendor. E-Check has also replaced the USSS Event Name Check System, which was an internal process used to determine suitability for an individual's access into USSS-protected events.

Overview

USSS is tasked by statute with coordinating physical security for NSSEs, in addition to providing protection for our nation's highest leaders.[1] The USSS Dignitary Protective Division (DPD) prevents and counters terrorist and criminal attacks on large events and their participants, which often include USSS protectees. DPD collects personally identifiable information (PII) in order to assess the criminal history of potential participants and make a security determination regarding whether to grant or deny them access to the events. Examples of participants are members of the media, vendors, volunteers, drivers, and other individuals who require access within a secured area.

The new event credentialing business process for participants (also referred to as applicants), used in conjunction with NSSEs and other large events attended by USSS protectees, is now partially outsourced to the Ardian Group, Inc. Ardian Group has been contracted to host a public website for applicants to initiate the credentialing. Prospective event applicants are provided with a web address to initiate the online application process to gain access to a specific large event. A designated Point of Contact (POC) typically serves as the coordinator for a specific group of applicants. The POC may either directly enter an applicant's required information into the Ardian Group application or provide a link for that applicant to enter his or her own data directly into the application.

Once the application process is initiated for an applicant, DPD is notified via email and subsequently initiates a manual process in which DPD authorized users log into the Ardian Group system and download applicant information. The downloaded report containing applicant information is then imported into E-Check to begin the security name check investigation process.

Once the security name check is completed, DPD requests the Ardian Group to produce event credentials for approved applicants.

[1] 18 U.S.C. § 3056(a) and (e), "Powers, authorities, and duties of the United States Secret Service."

E-Check has also replaced the USSS Event Name Check System in order to meet other protective and investigative needs of the USSS. In addition to its use in securing large events, E-Check is used on an as-needed basis, without Ardian Group, to process single or multiple names to determine suitability for entry into USSS-protected events of any size. E-Check automates the security name check process for authorized users. Authorized users establish a batch list of applicants under an event title. Once all the names have been established under an event, the entire list is imported into the E-Check system for processing in the same manner as for large events described above.

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 outsourcing of portions of the credentialing process for large events to Ardian Group. An applicant for a large event or designated POC is now initiating the online enrollment process through the Ardian Group website using a web-based application form. The online application process allows for secure and controlled collection of specific PII for entry into specific large events. Once the applicant passes various security name checks and is approved, badging credentials are generated to gain access to the specific large event. This PIA Update also discusses the replacement of the USSS Event Name Check System by E-Check.

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 participants will continue to be entered into E-Check in order to conduct appropriate security name 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)
- Photograph

Other PII that may be recorded in E-Check includes:

- Participant/Applicant and/or POC
  - 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. The USSS may try to resolve minor issues such as inconsistent name spellings, but generally, an inconsistent request will be returned to the requesting POC for clarification.

Uses of the Information

There are no changes in the uses of the information.

Data Retention by the project

Ardian Group deletes all PII data associated with an event within 15 business days of the conclusion of the event. The following activities are executed within the aforementioned time frame:

- All software administrators that do not require access for closeout activities and/or report generation are deleted from the application.

- All Ardian Group computers that were associated with the collection and/or processing of PII data are purged of any PII.
- All ancillary software used in the processing of PII data are purged.
- The database is destroyed; this action is not recoverable.
- The web application is destroyed. This includes the Uniform Resource Locator (URL) and Domain Name System (DNS).

The Ardian Group Office of Information Technology documents the date and time that the above activities are completed in their entirety.

Information Sharing

Ardian Group only captures the PII within their secure network and formats the data. Authorized DPD users then log into Ardian's secure network and capture the formatted data for submittal into E-Check. This PII data within Ardian's secure network is destroyed 15 days after the event concludes and is not shared further. As noted above, Adrian Group is required to purge all PII.

Redress

Access, redress, and correction 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 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 safety personnel. Individual applicants may only 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

Steve Sepulveda
Special Agent In Charge
Information Resources Management Division
Chief Information Office
United States Secret Service
Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

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