Privacy Impact Assessment Update
for the

Protective Intelligence eXchange

(PIX)

DHS/USSS/PIA-002(b)

July 3, 2019

Contact Point
Susan Goggin
Acting Special Agent in Charge
Protective Intelligence and Assessment Division
U.S. Secret Service
(202) 406-5731

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

Abstract

The United States Secret Service (Secret Service) renamed the Targeted Violence Information Sharing System (TAVISS) to the Protective Information eXchange (PIX) System. PIX is used to conduct name checks and determine whether an individual under investigation is of protective interest to any agency within the PIX community. The Secret Service is conducting this Privacy Impact Assessment (PIA) Update to reflect the name change and to describe additional personally identifiable information (PII) that was not previously collected by TAVISS but is now maintained in PIX by the Secret Service and participating agencies in the network.

Overview

PIX is a web-based information sharing tool designed to assist United States law enforcement agencies in assessing the risk of an unwanted outcome that an individual of interest[1] may pose. All users must be members of federal, state, or local law enforcement agencies engaged in protection pursuant to that agency's specific authorizing federal or state legislation. Information in PIX is contained in an internet-accessible database that includes the names and selected identifiers of persons subject to a protective intelligence investigation by one or more of the member agencies. This information is used to assist users in providing protective services to public officials.

The purpose of the system is to facilitate information exchange regarding individuals who have expressed an inappropriate interest in a public official. Individuals included in PIX may have threatened public officials, trespassed in protected facilities, or exhibited some other unusual behavior directed at a protected public official. Data in PIX is provided by participating law enforcement agencies and is derived from information obtained from their own investigations. This information is typically collected directly from the individual or through corroborative investigation of that individual.

PIX was designed to share a limited amount of information. Initially, a query/request for an individual's record is made by a law enforcement member based on personal identifiers or location. If a positive match on a query/request occurs in PIX, the querying user is directed to contact the record's originating agency to arrange for the exchange of further information according to each agency's protocols and policies. Authorized personnel of a PIX member agency may view, create, edit, and delete records established by their agency. All users may view records

[1] Individuals of interest who are included in PIX are chosen by the PIX member agencies based on their own criteria of protective interest. Typically, individuals of protective interest have made threats against public officials or exhibited an unusual behavior recognized to be outside the normal range of social behavior, such as attempting to circumvent security or expressing a persistent delusion related to a protected person or protected facility.

identified by querying specific data in the system, such as name or alias, as part of the information sharing program.

PIX member agencies are approved by the USSS. External (non-USSS) PIX users are users within a member agency and are authorized by an agency administrator who is approved by the USSS.

Reason for the PIA Update

The PIX PIA is being updated to reflect the system's name change and to describe the wider array of PII collected on individuals of protective interest to the Secret Service and participating agencies in the network. The additional PII will be discussed under Characterization of the Information.

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

The collection of PIX information is authorized by the Secret Service's protective and investigative authority contained in 18 U.S.C. §§ 3056 and 3056A.

The DHS/USSS-004 Protection Information System of Records Notice (SORN)[2] covers the collection of information necessary to implement protective measures and to investigate individuals who may come into proximity with a Secret Service protectee. The SORN also covers individuals who have been involved in incidents or events related to the protective functions of the Secret Service, and individuals who have sought to make contact with a protectee.

The PIX system has a System Security Plan congruent with National Institute of Standards and Technology (NIST) 800-53 Rev. 4 standards. The security plan was an integral part of the certification and accreditation package for the system to be granted approval to operate. The approval to operate was granted by DHS in April 2018 and expires April 2021.

PIX is subject to the Protective Intelligence eXchange (PIX) System Disposition Schedule N1-087-11-2, which requires records to be deleted when 5 years old or when the agency determines that the record is no longer needed. The schedule was amended on July 16, 2018, to reflect the system name change. This amendment has been endorsed by the Secret Service Chief Records

[2] DHS/USSS-004 Protection Information System, 76 FR 66940 (October 28, 2011).

Officer and was approved by the National Archives and Records Administration (NARA) on October 25, 2018.

Characterization of the Information

Any user authorized by a PIX member agency may establish PIX subject records using information obtained through direct observation; interviews with the subject or others; checks of government records; and research of open sources such as news media reports, websites, and social media.

Publicly available data may be used to obtain photographs, corroborate information collected through direct observation or interviews, and discover aliases so that PIX subject records can be more complete. Record completeness is necessary to improve the quality of results when users query the system.

A PIX subject record may consist of:

- Name;
- Alias (name, email, screen names, or other);
- Date(s) of birth;
- Sex;
- Race;
- Identifying Marks;
- Identifying numbers, including Social Security numbers (SSN), Federal Bureau of Investigation (FBI) number, state criminal identification numbers, prison identification numbers, Alien Registration number; passport number, and alternate identifying numbers;
- Address(es);
- Telephone number(s);
- Vehicle information;
- Photographs;
- Originating agency record number;
- PIX record number; and
- PIX user who established the record as well as the date and time of creation.

PIX subject records incorporate a wider array of PII than previously maintained in TAVISS. New PII datasets are: email and screen name, address(es), telephone number(s), vehicle information, photographs, and PIX record number.

Each PIX subject record also contains contact information for the PIX subject record's originating agency. Originating agency information includes:

- Agency name;
- Agency address;
- Agency point of contact (POC) name;
- Agency POC telephone number(s);
- Agency POC email address;
- Agency unit or squad name;
- Agency unit or squad supervisor name;
- Agency unit or squad supervisor title;
- Agency unit or squad telephone number(s); and
- Agency unit or squad email address(es).

Authorized PIX users may query PIX records based on subject record data. When a positive match (or hit) is obtained, then the user may use the agency information contained in the subject record to contact the originating agency via telephone or email and request additional information.

Privacy Risk: There is a privacy risk that that an individual's PII may be erroneously entered into PIX.

Mitigation: This risk is partially mitigated. System access is restricted to authorized Secret Service employees engaged in protective intelligence analysis or other authorized individuals of member law enforcement agencies. Of these authorized users, only a subgroup receives additional system rights allowing them to enter or edit records, which is a manual process. Limiting the number of users able to enter or edit records limits the risk of human error during data entry. Additionally, data is most often collected by law enforcement officers regarding the individual in the course of an investigation. The extent and accuracy of personally identifying information collected by this means depends on the individual's cooperation with investigators. Data may also be obtained lawfully from public or law enforcement records (e.g., existing PIX or other agency criminal/protective intelligence records).

Privacy Risk: There is a risk that more PII than necessary may be collected.

Mitigation: This risk is mitigated because authorized users collect only that PII that is necessary to enable USSS and PIX member agencies to carry out their protective and law

enforcement functions. USSS and member agencies enter only those individuals into PIX who have been subject to an authorized protective intelligence investigation. PII is collected to enable positive identification so that (a) the individual is identifiable during future interactions with the agency, (b) the individual is not erroneously identified as, or linked to, another individual, and (c) further investigation can be conducted (if necessary).

Uses of the Information

There are no changes in the uses of the information. The information collected in this system is intended to be shared with participating law enforcement agencies for their investigative use to assist in mitigating potential threats to protected persons.

Within DHS, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, and the Federal Protective Service are active member agencies.

Notice

Notice remains unchanged with this update; the information comprising a PIX record is collected from the reporting law enforcement agency's records, as such the individual is not on notice of the creation of a PIX record.

Data Retention by the project

PIX is subject to N1-087-11-2 Protective Intelligence eXchange (PIX) System, which was amended on July 16, 2018, to reflect the system name change. Records are deleted after 5 years, or when the agency determines that they are no longer needed. This amendment has been endorsed by the Secret Service Chief Records Officer and was approved by NARA on October 25, 2018.

Information Sharing

There have been no changes with internal and external sharing and disclosure.

Redress

As a protection information system owned by the Secret Service, the DHS/USSS-004 Protection Information System SORN includes exemptions from the access and redress provisions of the Privacy Act. However, access requests will be considered on a case-by-case basis if made in writing to the Secret Service's FOIA Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington DC 20223, as specified in the DHS/USS-004 SORN. Although

redress may not be available through the Secret Service because PIX is an index to participating agencies' records, an individual of record may contest the accuracy and seek the correction of any data with the originating agency through that agency's published mechanisms.

Auditing and Accountability

The information is shared between the U.S. Secret Service and other participating agencies. The U.S. Secret Service bears responsibility for the security of PIX data. The storage and transmission of any sensitive information shared with organizations outside the Secret Service is required to be appropriately secured pursuant to the Office of Management and Budget M-07-15, Protection of Sensitive Agency Information. In addition, five primary security standards were applied to PIX:

- Identification/Authentication – PIX uses two-factor user identification. Internal users of PIX must use PIV cards/credentials to access the system. External users authenticate to an Identity Domain Provider (IDP) and are authorized by the PIX application.
- Auditing/Integrity – PIX records user activity for after-the-fact investigation of transactions made by any user.
- Accountability – Security-relevant activities on PIX are traced to users who may then be held responsible for their actions. The type of event, time, source and user associated, and unauthorized changes are captured by USSS Systems Engineering (SE) and reviewed by PIX.
- Access Control/Confidentiality – PIX operating procedures limit access to authorized programs. User access control is approved/disapproved by an appointed manager in USSS Protective Intelligence & Assessment Division (PIAD).
- Non-Repudiation – Any actions or changes can be associated with the user who made them, preventing a denial in an electronic message or action and proving delivery or origin of information transactions. The PIX system records all user information with timestamps that cannot be altered. All user activity is tied to the specific user account.

Authorized PIX users from member agencies must have an active user account with an IDP. The basic criteria for membership is that a participating agency must be a federal, state, or local law enforcement entity and be engaged in dignitary protection or directly supporting a protective detail by conducting protective intelligence investigations. Agencies must complete an application that is reviewed for eligibility by an appointed manager within PIAD. If access is approved, the System Administrator within PIAD contacts the agency point of contact and requests the appointment of a member agency administrator. The member agency administrator is

responsible for adding and removing agency users upon request, duty and assignment change, and termination.

Responsible Official

Susan Goggin
Acting Special Agent in Charge
Protective Intelligence & Assessment Division
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