



**Privacy Impact Assessment
for**

Targeted School Violence Database

DHS/USSS/PIA-027

April 9, 2020

Contact Point

Diana Drysdale

National Threat Assessment Center (NTAC)

Office of Strategic Intelligence and Information (SII)

(202) 406-6362

Reviewing Official

Dena Kozanas

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The United States Secret Service (Secret Service or USSS) has created the Targeted School Violence database as part of an ongoing research project that examines past incidents of targeted violence directed at or on the immediate property of a K-12 school or an institute of higher education (IHE). These incidents include both averted and actual attacks. The purpose of the project is to analyze the information collected to develop best practices for preventing incidents of targeted school violence. The findings will be released in a report and incorporated into a national training initiative for those with school safety responsibilities. The Secret Service is conducting this Privacy Impact Assessment (PIA) to evaluate the privacy risks associated with the Targeted School Violence database collection of personally identifiable information (PII).

Overview

The U.S. Secret Service has a longstanding tradition of conducting threat assessments as part of its mandate to ensure the safety of this Nation's highest elected officials. The National Threat Assessment Center (NTAC) is dedicated to the USSS protective mission by expanding the field of violence prevention with a particular focus on the prevention of targeted school violence. The Secret Service was authorized by the Presidential Threat Protection Act of 2000 to establish the National Threat Assessment Center (NTAC) to perform research, training, information sharing, and consultation on threat assessment and the prevention of targeted violence in support of federal, state, and local law enforcement entities.¹ The term 'targeted violence' refers to a certain type of non-random violence that can take place within different contexts, including school-based attacks, workplace violence, stalking, acts of terrorism, and attacks that target government entities. To provide research and training, NTAC performs behavioral analyses of past incidents of targeted violence.

At the request of the Director of the U.S. Secret Service, and subsequently the Secretary of the Department of Homeland Security (DHS), NTAC initiated a two-part project that included: (1) issuing an operational guide for using threat assessment to prevent school-based acts of targeted violence (released July 2018); and (2) conducting a new study of school-based attacks.² This study would build on the Secret Service's previous research known as the Safe School Initiative (SSI).

The Targeted School Violence database is a working research tool used specifically for this study. The purpose of the project is to analyze the information collected to develop best practices

¹ Pub. L. 106-544, § 4; 18 U.S.C. § 3056 note.

² U.S. Secret Service, Department of Homeland Security, National Threat Assessment Center, "Enhancing school safety using a threat assessment model: An operational guide for preventing targeted school violence," *available at* https://www.secretservice.gov/data/protection/ntac/USSS_NTAC_Enhancing_School_Safety_Guide_7.11.18.pdf.



for preventing incidents of targeted school violence. In order to perform the required statistical analyses (e.g., frequencies, Chi squares, significance tests), data is exported from the database to statistical software products. NTAC does not use any Advanced Analytics or Machine Learning tools.

This project is in direct support of NTAC's mission to conduct research and training on the prevention of acts of targeted violence. Behavioral research on targeted violence further informs the threat assessment techniques NTAC develops that are customized and shared across contexts. The findings will be released in a public report and incorporated into a national training initiative for those with school safety responsibilities.

The Targeted School Violence database contains PII on the perpetrators of plots and attacks retrieved from a variety of sources, both open source and law enforcement sensitive. The open source information comes from media reports; books; publicly-available social media; case law; court filings; publicly released law enforcement, government, or court files; and other public records available in Lexis-Nexis, Accurint, TLO.com, and Courtlink. The law enforcement information comes from reports and transcripts from law enforcement agencies, the courts, and other government agencies that were not publicly released. This other category of information may include material deemed Law Enforcement Sensitive (LES) or For Official Use Only (FOUO). In some cases, NTAC has signed court documents to keep that information restricted to NTAC use only.

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?

Information is solicited and obtained under the authority of 18 U.S.C. § 3056 Powers, Authorities, and Duties of United States Secret Service; 18 U.S.C. § 3056A Powers, Authorities, and Duties of the United States Secret Service Uniformed Division; and the Presidential Threat Protection Act of 2000 (Pub. L. 106-544, § 4) (18 U.S.C. § 3056 note).

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

The Protection Information Systems SORN³ describes the Secret Service's collection and maintenance of records to assist in safeguarding its protectees, including information on

³ DHS/USSS-004 Protection Information System of Records, 76 FR 66940 (October 28, 2011). USSS is in the process of updating this SORN to more clearly describe the collection of records associated with this program.



individuals who have been involved in incidents or events that relate to the protective functions of the USSS. This SORN includes these records and their associated routine uses for the purposes of designing and implementing protective measures, furthering threat assessment and targeted violence prevention activities, and exercising other USSS protective functions.

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

No, Authority to Operate is pending approval of this PIA.

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

Permanent records of Protective Intelligence Research files produced by NTAC are covered under NARA Disposition Schedule N1-87-88-1, item 2E1. These items consist of internal and external studies, proposals, and contracts pertaining to behavioral sciences research on assessments of dangerous prediction of violence and development of research models relating to the agency protective function. The records are permanently retained for 20 years and then transferred to the custody of the National Archives.

A new DHS Enterprise Schedule designed to standardize retention of investigative records across the Department and its components is currently pending review by NARA. This pending schedule may extend some retention periods, once approved and issued. NTAC research records are currently being reviewed for inclusion in this DHS Enterprise Schedule.

Additionally, NARA General Records Schedule 5.2, Transitory and Intermediary Records, cover all non-recordkeeping copies of electronic records maintained in email systems, computer hard drives or networks, web servers, or other locations after the recordkeeping copy has been copied to a recordkeeping system or otherwise preserved.

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.

The information that will be collected by NTAC is not covered by the Paperwork Reduction Act because NTAC does not directly collect information from the individual. USSS Field Offices across the United States worked with their local law enforcement partners to acquire investigative case files, including police investigative records, publicly available court records, and other publicly available information.



Section 2.0 Characterization of the Information

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

The Targeted School Violence database contains information regarding the perpetrators and targets of acts of violence directed toward K-12 schools and IHEs.⁴

Perpetrator data includes:

- Name;
- Date of birth (DOB);
- Gender;
- Grade in school;
- Residence at the time of the incident;
- Criminal and behavioral history (including mental health symptoms and treatment, as well as substance use/abuse) synthesized from diverse sources, such as police investigative records, publicly available court records, and other publicly available information source materials;
- Court records;
- School records obtained from police investigative records, publicly available court records, and other publicly available information source materials; and
- Narrative description of the incident perpetrated.

Data on target(s) includes:

- Name;
- Age at the time of the incident; and
- Gender.

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

Information is collected from a variety of sources, both open source and law enforcement sensitive. These sources include police investigative records, publicly available court records, and

⁴ The names of minors will only be used by NTAC if the names were previously identified in the media or if the information is otherwise public knowledge.



other publicly available information. These source materials may also contain school records and mental health records. Obtained records may include interviews with the attackers, interviews with witnesses and people who knew the attackers, school transcripts and disciplinary histories, social media screen captures, data from the searches of phones and computers used by the attackers, the results of searches of the attackers' residences, personal journals and other writings, and court records containing the results of mental health evaluations both before and after the attacks.

The open source information, which is manually collected by NTAC staff, comes from media reports; books; social media; case law; court filings; publicly released law enforcement, government, or court files; and other public records available in Lexis-Nexis, Accurint, TLO.com, and Courtlink. The non-open source information is from reports and transcripts from law enforcement agencies, the courts, and other government agencies that were not publicly released. It was collected by directly contacting the various court clerks, prosecutors, and law enforcement agencies who then shared the information with NTAC. This other category of information may include information deemed LES or FOUO. In some cases, NTAC signed court documents to keep that information restricted to NTAC use only.

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

Yes. The Targeted School Violence database uses open source information obtained from commercial databases, such as LexisNexis, Accurint, TLO.com, and CourtLink, as well as other publicly available information. The information is synthesized with other open source information as well as the non-open source information to document details of past incidents of violence and inform research on the prevention of future acts of targeted violence.

2.4 Discuss how accuracy of the data is ensured.

NTAC researchers check the information obtained from open sources against the non-open source information before it is entered into the database. Multiple layers of review are applied to every stage of the project to ensure accuracy and reliability of reported findings. The established research protocol includes two levels of review to ensure the final record accurately reflects what was reported in all the sources.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that the Targeted School Violence database could collect and report inaccurate information.



Mitigation: The risk is mitigated by comparing all information with the non-open source reports and by training NTAC personnel to assess the facts as they are reported and accurately reflect the source (i.e., “court records reported...” or “family members told the media...”). Furthermore, the established research protocol includes two levels of review to ensure the final record accurately reflects what was reported. The case is initially researched and “authored” by a staff member. The file is then reviewed by a senior staff member who also performs his or her own research to fill information gaps to ensure clarity and verify accuracy.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The information in the Targeted School Violence database is used to study the phenomenon of acts of targeted violence in schools as part of the DHS priority to enhance school safety for our nation. It further enhances the Agency’s level of knowledge in the area of threat assessment by analyzing individual plots, attempted attacks, and attacks on our schools. The collection of PII, such as the perpetrators’ name, age, and gender, is necessary as there are developmental issues at play that affect the behavioral analysis used to formulate threat assessment principles. It is also often the only way to ensure there is no duplication of incidents and/or perpetrators. The information contained in the database is also used to develop training modules, a key element in the performance of NTAC’s training mission. Omitting key information from these often well-known incidents would compromise the Secret Service’s credibility and the effectiveness of the training.

Information about the perpetrators’ residence at the time of the incident, criminal history, and behavioral history must be included to not only test current threat assessment theories but also to identify, develop, and test new theories that directly impact how the Secret Service and others trained by USSS with protective responsibilities in our communities conduct threat assessments of persons of concern to prevent potential acts of targeted violence.

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.

No.



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

No. There are no other 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 risk that the information collected could inaccurately identify lawful behavior as suspicious and form the basis of a behavioral analysis.

Mitigation: This risk is mitigated by training NTAC personnel to record only information that is both credible and necessary in the furtherance of the Secret Service's protective mission. Further, NTAC personnel are trained to identify best practices in threat assessment in order to help prevent acts of targeted violence. Threat assessment itself is not a criminal investigation and does not focus on the identification and labeling of behaviors as lawful or not. Rather, it is about identifying those behaviors that would or should cause concern, not in isolation, but in the context of a person's life.

Section 4.0 Notice

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

The Protection Information System SORN⁵ provides notice regarding the collection of information and the routine uses associated with the collection of the information. A majority of open source information is not collected directly from the individual; therefore, there are no opportunities for directly providing notice. Additionally, notice to individuals prior to collection of information could impede law enforcement's investigation. The final rule for the system of records officially exempts the system from portions of the Privacy Act. This PIA serves as public notice of the existence of the Targeted School Violence database and the type of information that it collects.

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

There is no opportunity to decline or opt-out of the agency processes that use this database.

⁵ DHS/USSS-004 Protection Information System of Records, 76 FR 66940 (October 28, 2011).



4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that subjects of the research may not know that information about them is being collected and maintained, or fully understand how USSS uses this information.

Mitigation: This risk is partially mitigated. USSS provides some notice that perpetrators of school shootings may be in this database; however, the notice is general. The NTAC website provides information to the public about the mission and activities of the NTAC, and NTAC's published "Protecting America's Schools" report tells the public how this information is used.

Section 5.0 Data Retention by the project

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

Retention for permanent records maintained by the Targeted School Violence database is covered under NARA Disposition Schedule N1-87-88-1, item 2E1. These records are transferred to the permanent custody of the National Archives after 20 years.

A new DHS Enterprise Schedule designed to standardize retention of investigative records across the Department and its components is currently pending review by NARA, which once approved and issued may change some of the retention periods. NTAC research records are currently being reviewed for inclusion in this DHS Enterprise Schedule.

Additionally, NARA General Records Schedule 5.2, Transitory and Intermediary Records covers all non-recordkeeping copies of electronic records maintained in email systems, computer hard drives or networks, web servers, or other location after the recordkeeping copy has been copied to a recordkeeping system or otherwise preserved.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be retained for longer than is required or needed in the Targeted School Violence database.

Mitigation: The Secret Service mitigates this risk by only retaining information in the Targeted School Violence database for the timeframes outlined in Section 5.1 consistent with general record retention schedules and necessary to complete the USSS mission.



Section 6.0 Information Sharing

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.

No. The Secret Service does not share information directly from the Targeted School Violence database. The data collected by USSS and included in the Targeted School Violence database is only used by NTAC staff to generate statistics and other content and to author reports that analyze the incidents of targeted violence. At the completion of the data collection and analysis, a report will be issued and publicly released with the findings of the study. The data is also used for developing training modules focused on preventing acts of targeted violence.

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

The Agency does not share information directly from the Targeted School Violence database.

6.3 Does the project place limitations on re-dissemination?

No. Information in the database is not shared with any personnel outside of NTAC or the project contractors. The only dissemination is through the reports and training modules described in Section 6.1. Further, files are maintained on the USSS servers, which is restricted to NTAC employees and contractors.

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

Information in the Targeted School Violence database is not shared with any entity outside of NTAC.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: To the extent that information may be released pursuant to any routine uses, there is a privacy risk that PII may be disclosed to an unauthorized recipient.

Mitigation: To mitigate this risk, disclosure may occur only by authorized USSS employees in the furtherance of their respective duties. Authorized USSS employees may only share information pursuant to routine uses specified in DHS/USSS-004 Protection Information System of Records SORN listed in Section 1.2 when compatible with the purpose for which the information was collected.



Section 7.0 Redress

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

As a protection information system owned by the Secret Service, the DHS/USSS-004 Protection Information System SORN permits certain portions of the Targeted School Violence database to be excluded from the access and redress provisions of the Privacy Act. However, access requests from U. S. Citizens and Lawful Permanent Residents will be considered on a case-by-case basis if made in writing to the Secret Service's Freedom of Information Act (FOIA) Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223, as specified in the Protection Information System SORN. Individuals, regardless of citizenship or legal status, may also request access to their records under FOIA. Instructions for filing a FOIA or PA request are available at <http://www.secretservice.gov/press/foia>.

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

The procedures are the same as those outlined in Question 7.1.

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

The mechanism for requesting correction of information contained in any Secret Service protection information system is specified in the DHS/USSS-004 Protection Information System SORN, in this PIA, and is also available on the Secret Service's public webpage.

7.4 Privacy Impact Analysis: Related to Redress

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

Mitigation: The Secret Service mitigates this risk by permitting individuals to request access to information about themselves under the FOIA and Privacy Acts. The nature of the Targeted School Violence database and the information it collects and maintains is such that the ability of individuals to access or correct their information may be limited by Privacy Act exemptions. The redress and access measures offered are appropriate given the purpose of the system, which is to collect, analyze, and store information collected on the perpetrators and past incidents of targeted violence directed toward K-12 schools or IHEs.



Section 8.0 Auditing and Accountability

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

As the Targeted School Violence database is a working research product, all NTAC employees and contractors have access to the project's data files, such as MS Access and SPSS, as part of their daily work and responsibilities. Since this work involves completing and verifying the accuracy of the information it contains, the project staff is constantly reviewing the content.

All Secret Service information systems are audited regularly to ensure appropriate use of and access to information. Specifically related to this system, application access is mediated through a two-tier identification and authentication process.

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

All Secret Service employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. Also, 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?

Access to the Targeted School Violence database is restricted to NTAC employees and contractors, who all require access to perform their work, namely the identification and research of the incidents of targeted violence it contains.

DHS Sensitive Systems Policy Directive 4300A outlines information technology procedures for granting access to Secret Service computers. Access to the system is strictly limited by access controls to those Secret Service employees who have a legitimate need-to-know in the furtherance of their role in behavioral analysis.



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?

All information sharing agreements, MOUs, and new uses of information are to be reviewed by the USSS Privacy Services Program, Office of Chief Counsel, and the respective program office.

Responsible Officials

Frederick Sellers
Assistant Director
Office of Strategic Intelligence and Information
U.S. Secret Service

Approval Signature

[Original, signed copy complete and on file with the DHS Privacy Office]

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security