Privacy Impact Assessment
for

Comprehensive Incident Database on Targeted Violence (CID-TV)

DHS/USSS/PIA–021

May 4, 2018

<u>Contact Point</u>
Diana Drysdale
National Threat Assessment Center (NTAC)
Office of Strategic Intelligence and Information (SII)
(202) 406-6362

<u>Reviewing Official</u>
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) United States Secret Service (Secret Service or USSS) has created the Comprehensive Incident Database on Targeted Violence (CID-TV). CID-TV is an on-going research project that analyzes past incidents of targeted violence directed toward public officials, public figures, and prominent facilities, structures, or events in support of the mission of the National Threat Assessment Center (NTAC), Office of Strategic Intelligence and Information (SII). The Secret Service is conducting this Privacy Impact Assessment (PIA) to evaluate the privacy risks associated with CID-TV collecting personally identifiable information (PII).

Overview

USSS was authorized by the Presidential Protection Act of 2000[1] to establish the 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. 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. Since no resource previously existed to identify and describe past incidents of targeted violence against government entities, the Secret Service created the Comprehensive Incident Database on Targeted Violence (CID-TV).

CID-TV contains descriptive information relevant to threat assessment research on past plots and attacks directed toward public officials and facilities, as well as nationally prominent public figures and spaces (e.g., major monuments, landmarks, attractions, and events). As the research and training supports federal, state, and local law enforcement, CID-TV includes plots and attacks at all levels of government. Entries range from Secret Service protective interests (e.g., foreign dignitaries, the United Nations General Assembly, the White House, the President of the United States) to local targets (e.g., mayors, town halls, police officers).

CID-TV contains personally identifiable information (PII) on the perpetrators of plots and attacks retrieved exclusively from open sources, including news, case law, social media, books, NewspapersArchive.com, and open searches of the internet. CID-TV also contains public records available in LexisNexis, Accurint, TLO.com, CourtLink, and other public records available from government entities via the internet.

[1] Pub. L. 106-544, § 1(a)(4), 114 Stat. 2763 (2000).

With this working research tool, NTAC is able to identify and analyze different subsets of incidents to examine various threat assessment questions. CID-TV also aids in the identification of trends, new areas of research, and streamlines the research process. Ultimately, NTAC researchers use data from CID-TV to author reports and prepare training modules focused on preventing acts of targeted violence. Modules and reports may be disseminated outside the Agency. The first report, "*Attacks on Federal Government 2001-2013: Threat Assessment Considerations*"[2] was released in December 2015. Future reports will cover attacks on government at the state and local level as well as attacks on nationally prominent attractions and events. In order to perform the statistical analyses needed for these reports, data is exported to separate working files in Microsoft (MS) Access and the advanced statistical software package, IBM SPSS Statistics.

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 Protection Act of 2000 (Pub. L. 106-544, § 1(a)(4), Dec. 21, 2000, 114 Stat. 2763).

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

The Protection Information Systems SORN[3] describes the Agency's collection and maintenance of records to assist in protecting its protectees, including information on individuals who have been involved in incidents or events which relate to the protective functions of the USSS.

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

Yes. Authority to Operate will expire on November 28, 2019.

[2] *Available at* https://www.secretservice.gov/data/protection/ntac/Attacks_on_Federal_Government_2001-2013.pdf.
[3] DHS/USSS-004 Protection Information System of Records, 76 FR 66940 (October 28, 2011).

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 CID-TV 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 and when 20 years old, are transferred to the custody of the National Archives.

However, a new DHS Enterprise Schedule designed to standardize retention of investigative records across the Department and its Components is currently pending review by the National Archives and Records Administration and may affect some of the retention periods, once approved and issued. NTAC research records are currently being reviewed for inclusion in this DHS Enterprise Schedule. The proposed retention schedule states Protective Intelligence Research project files are permanently retained and when 30 years old, are transferred to the custody of the National Archives. Also, Protective Intelligence Research administrative and support files are temporarily retained, and should be destroyed when business use ceases.

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 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 CID-TV is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

CID-TV contains information regarding the perpetrators and targets of acts of violence directed toward public officials, figures, facilities/sites, and spaces that are nationally prominent.

Unique numbers are generated for incidents, subjects, and targets; and information is retrievable by these numbers.

Perpetrator(s) data includes:

- Name;
- Age at the time of the incident;
- Gender;
- Highest educational level attained;
- 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 reports available in open source;
- Court records, and
- Narrative description of the incident perpetrated as reported by open sources.

Target(s) data includes:

- Name;
- Gender;
- Title at the time of the incident; and
- Organization at the time of the incident.

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

Open source information is manually collected by NTAC researchers on the perpetrator(s) and target(s) of the incidents of targeted violence cataloged. The sources of information are exclusively from open-sources, including news, case law, social media, books, NewspapersArchive.com, and open searches of the internet. Information is also obtained from public records available in LexisNexis, Accurint, TLO.com, CourtLink, and government entities (such as local courts) via the internet. All information collected by USSS is open source.

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. CID-TV uses open-source information exclusively. The information obtained from commercial databases, such as LexisNexis, Accurint, TLO.com, CourtLink, and NewspapersArchive.com, is publicly available information. The information is synthesized with other open source information, such as the news media, to document details of past incidents of violence and inform research on the prevention 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 other open source information before it is entered into the database. The established research protocol includes three levels of supervisory review to ensure the final record accurately reflects what was reported in the open sources used.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that CID-TV collects and reports inaccurate information.

Mitigation: The risk is mitigated because NTAC personnel are well trained to negotiate the facts reported and accurately reflect the source (*i.e.*, "court records reported…" or "family members told the media…"). All NTAC reports indicate the data collected is available via open sources. Furthermore, the established research protocol includes three levels of review to ensure the final record accurately reflects what was reported in the open sources used. 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. Lastly, a second senior staff member reviews the file for any discrepancies.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The information in CID-TV is used to enhance the Agency's level of knowledge in the area of threat assessment by analyzing individual plots, attempted attacks, and attacks on public interests. PII, such as the perpetrators' and targets' name and gender, are necessary as that information is the only way to ensure there is no duplication of incidents and/or perpetrators entered into the database. The information in CID-TV is also used to develop training modules, a key element in the performance of NTAC's training mission. Omitting key information for these often well-known incidents would compromise the Agency's credibility and the effectiveness of the training.

Information about the perpetrators' age at the time of the incident, highest educational level attained, residence at the time of the incident, and criminal and behavioral history must be entered into CID-TV to not only test current threat assessment theories, but also to identify, develop, and test new theories that directly impact how the Agency 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 privacy risk that the information contained in CID-TV could inaccurately identify lawful behavior as suspicious and form the basis of a behavioral analysis.

Mitigation: This risk is mitigated. NTAC researchers check the information obtained from open sources against other open source information before it is entered into the database and are trained to record only that information that is both credible and necessary. The established research protocol includes three levels of supervisory review to ensure the final record accurately reflects what was reported in the open sources used.

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 SORN[4], provides notice regarding the collection of information and the routine uses associated with the collection of the information. Notice to individuals prior to collection of information could impede law enforcement's investigative activities. The final rule for the system of records officially exempts the system from portions of the Privacy Act. Moreover, this PIA serves as public notice of the existence of CID-TV and the type of information that it collects. Further, all data is gathered from open source information.

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

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. As stated above, all information is gathered from open sources, as opposed to directly from the individual.

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: USSS partially mitigates this privacy risk by providing notice to subjects, who are perpetrators and targets of acts of violence, through publishing this PIA and the associated Protection Information System SORN. Additionally, the CID-TV PIA lists potential sources used to collect open-source information to increase transparency, thereby informing users from where USSS collects certain information.

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 CID-TV is covered under NARA Disposition Schedule N1-87-88-1, item 2E1. These records are transferred to the permanent custody of the National Archives once they become 20 years old.

However, a new DHS Enterprise Schedule designed to standardize retention of investigative records across the Department and its Components is currently pending review by the National Archives and Records Administration that may change some the retention periods, once approved and issued. NTAC research records are currently being reviewed for inclusion in this DHS Enterprise Schedule. The proposed retention schedule states Protective Intelligence Research project files are permanently retained and when 30 years old, are transferred to the custody of the National Archives. Also, Protective Intelligence Research administrative and support files are temporarily retained, and should be destroyed when business use ceases.

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 CID-TV.

Mitigation: The information in CID-TV will be retained for the timeframes outlined in Section 5.l 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.

The Agency does not share information directly from CID-TV. The data collected by USSS and uploaded into CID-TV is only used by NTAC staff to generate statistics and other content, and to author reports that analyze the incidents of targeted violence in CID-TV. The first report, "*Attacks on Federal Government 2001-2013: Threat Assessment Considerations*,"[5] was released publicly in December 2015. Future reports will cover attacks on government at the state and local level as well as attacks on nationally prominent attractions and events. 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 CID-TV.

6.3 Does the project place limitations on re-dissemination?

No. Information in the MS Access and SPSS files is not shared with any personnel outside of NTAC. The only dissemination is through the reports and training modules described in question 6.1. Further, MS Access and SPSS files are maintained on the USSS shared drive, which is restricted to NTAC employees within the Secret Service.

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

Information in CID-TV is not shared with any entity outside of NTAC.

[5] *Available at* https://www.secretservice.gov/data/protection/ntac/Attacks_on_Federal_Government_2001-2013.pdf.

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 be made 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 Protection Information System SORN.

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 Protection Information System SORN permits certain portions of CID-TV to be excluded from the access and redress provisions of the Privacy Act (PA) and those of the Judicial Redress Act. However, access requests from U. S. Citizens and Lawful Permanent Residents, as well as those covered by the Judicial Redress Act, 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. If compliance with a request would not interfere with, or adversely affect the accomplishments of the Secret Service's protective and investigatory mission, information contained within this system may be released or amended. 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 Protection Information System SORN, in this PIA, and 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: Individuals can request access to information about themselves under the FOIA and Privacy Acts and may also request that their information be corrected. The nature of CID-TV 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 perpetrator(s) and past incidents of targeted violence directed toward public officials, public figures, and prominent facilities/structures/events. However, requests to amend records will be considered on a case-by-case basis if made in writing to the Secret Service's FOIA/PA Officer, Communications Center (FOIA/PA), 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223.

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 a working research product, all NTAC employees have access to the project's MS Access and SPSS files as part of their daily work and responsibilities. As 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, through the use of PIV cards, unique PINs, and individual access to the shared drive. Any changes to the hardware or software configuration are subject to review and approval by the USSS Configuration Control Board process to ensure integrity of the application.

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 CID-TV is restricted to NTAC employees, who all require access to perform their work, namely the identification and research of the incidents of targeted violence it contains.

DHS physical and information security policies dictate who may access USSS computers and filing systems. Specifically, 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 reviewed by the USSS Privacy Office, 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 on file with the DHS Privacy Office]

____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security