Privacy Impact Assessment
for the

FSD Polygraph System

DHS/USSS/PIA-007

December 15, 2011

Contact Point
Craig Hutzell
U. S. Secret Service
202-406-6800

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Forensic Services Division (FSD) Polygraph Branch of the United States Secret Service (USSS) uses the FSD Polygraph system to track all polygraph examinations that it administers. This database contains information on applicant and criminal polygraph examinations and their results. USSS is conducting this Privacy Impact Assessment (PIA) because this system contains personally identifiable information (PII) of individuals who undergo an exam.

Overview

The FSD Polygraph System is a shared system that can be accessed only by the eight polygraph examiner quality control (QC) personnel assigned to the Operations Section. USSS administers polygraph tests to five categories of individuals: (1) applicants for USSS employment to demonstrate eligibility; (2) USSS subjects of federal allegations of criminal activity who agree to the exam in connection with their charges; (3) subjects of federal agency Offices of Inspector General (OIG) criminal investigations who agree to the exam in connection with their charges; and (4) subjects of allegations in state and local law enforcement matters, or at the request of the National Center for Missing and Exploited Children, to provide forensic and investigative support in any investigation involving missing or exploited children pursuant to 18 U.S.C. § 3056(f); and (5) subjects of allegations in state and local law enforcement investigations involving other major felonies.

In all instances the individual has consented to the use of the polygraph. A Statement of Consent is presented to the examinee and must be voluntarily executed. At any time during the polygraph, the examinee may opt to terminate the examination. USSS interprets its authority to allow it to polygraph anyone who consents.

With respect to federal agency OIG requests for polygraph support, there is a Memorandum of Understanding between USSS and the relevant OIG, and OIG requests are vetted through the USSS Office of Professional Responsibility and the USSS Inspection Division for authorization. For any other exams run for any other federal, state, or local agency, the exam will not be run in internal affairs/administrative cases. USSS polygraph examinations for federal, state, and local agencies, other than OIGs, are quite infrequent and are conducted only for those agencies that do not have existing polygraph programs. As such, they are conducted in the absence of any MOU/MOA's using the same approval process as for OIG.

Examiners use the FSD Polygraph System to search, track, and monitor the program's productivity pursuant to that agency's specific authorizing federal or state legislation and the rules and regulations applicable to law enforcement agencies.

A typical transaction is an applicant for employment at USSS voluntarily submits to a polygraph examination. Information is collected directly from the examinee at this time. The information provided in response to the questions is input into FSD Polygraph System by the polygraph examiner. Information that is input into the system can then be reviewed, searched, and updated only by QC examiners. A QC examiner has the capability to search the system by entering a simple search (name, date of birth, and/or identification number) or an advanced search (last name, first name, middle name, date of birth, sex, race, and/or SSN). The user may also limit their search to those records containing partial data they have available and can modify the search with Boolean logic. This system does not maintain criminal history,

mental health records, or any other such information regulated by disclosure restrictions. Instead, it merely serves as a method to quickly determine whether an individual has been administered a polygraph by USSS and if so, shows the outcome of the exam.

The FSD Polygraph System was designed to maintain a limited amount of information in order to expedite access to outcomes, dates of exams, and pertinent data pertaining to an individual polygraph without having to manually search files in archives. Case files, including questions answered and responses provided, are maintained in paper form in a vault separate from this system.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

The information collected includes the names and identifiers of individuals who have applied for employment at USSS or are subjects of allegations of financial crimes who agree to the polygraph exam in connection with their charges.

The system may contain any of the following data on a subject:

- Name (first, middle, last)
- Date of birth
- ID number
- SSN
- Office of Origin
- Exam date
- Exam status Test results (i.e., Deception Indicated; No Deception Indicated; Inconclusive)
- Case Number

Case files, including questions answered and responses provided, are maintained in paper form in a vault separate from this system.

1.2 What are the sources of the information in the system?

The information in the FSD Polygraph System is input by QC examiners based on information provided in the applicant's *Questionnaire for National Security Positions* (SF-86), or based on information gathered by the administering polygraph examiner through the interview of the examinee.

1.3 Why is the information being collected, used, disseminated, or maintained?

This information is being collected, used, disseminated, or maintained to assist USSS and participating agencies in fulfilling their investigative and hiring missions by monitoring progress of individuals in the hiring system, as well as to support agents and law enforcement agencies for whom criminal tests are conducted on subjects of allegations of criminal activity.

1.4 How is the information being collected?

Only a QC examiner working in the Polygraph Operations Branch may enter data or access the database.

1.5 How will the information be checked for accuracy?

The accuracy of the information submitted is the responsibility of the QC examiners, who receive extensive training on administering these tests to ensure accuracy.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The collection of the information is authorized by the Federal Records Act, 44 U.S.C. § 3101, and the Secret Service's protective authority contained in 18 U.S.C. §§ 3056 and 3056A.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: There is a privacy risk that more information may be collected than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: USSS minimizes the risk in two ways. First, the information related specifically to the questions and answers provided during the exam are maintained in paper form and destroyed after a period of time so as to minimize the number of individuals with access to this information. Additionally, USSS minimizes this risk by collecting and entering the minimum amount of information on only those individuals who have been authorized for polygraph testing subject to an authorized law enforcement investigation or who are applicants requiring examination. USSS maintains only the results of the exam within this system.
Privacy Risk: There is a risk of erroneous entry of an individual's PII into the Polygraph database.

Mitigation: The Polygraph Branch mitigates this risk by limiting input and access to the system to authorized USSS QC examiners engaged in applicant tracking or the quality control process.

Privacy Risk: There is a risk that the information from the questions and answers could be incorporated into the IT system.

Mitigation: The IT system was developed so that it does not have a field to allow such information to be incorporated into it. The questions and answers are maintained only in paper form.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe the uses of information.

The information collected in this system is intended to be shared with internal divisions of USSS for applicability in the employment application process, or with other law enforcement agencies for their investigative use on exams based upon criminal allegations. The criminal examination data is shared between the Secret Service and other participating accredited law enforcement agencies. It should be noted that applicant PII and criminal suspect PII are kept in two separate areas of the database. Applicant PII is internal and used/disseminated only within the USSS for applicant processing.

Authorized users in the USSS query the database for names of individuals that come to the attention of the USSS because they (1) have been administered a polygraph examination as part of the pre-employment process, or (2) have been administered a polygraph examination concerning a specific criminal act or accusation.

2.2 What types of tools are used to analyze data and what type of data may be produced?

No tools are used to analyze the data in or produced from this system.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not directly use any publicly available data. All data provided is entered by QC examiners who acquire information in the course of investigations, which may or may not include information from publicly available sources.

Case files, including questions answered and responses provided, are maintained in paper form in a vault separate from this system.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: The privacy risk associated with the uses of the information is that users may use the information for reasons not consistent with the original purpose.

Mitigation: To mitigate this risk, access is limited to those within the polygraph branch quality control process with the responsibility to limit conveyance of information to only those

employees with a need-to-know for their job function (i.e., managing or conducting investigations of individuals suspected of crimes or in the application). All users are required to affirmatively acknowledge the following responsibilities regarding the use and dissemination of polygraph records:

- Records are law enforcement sensitive and should not be accessed by or disseminated to non-members;
- Any unauthorized access may be subject to criminal and civil penalties;
- Information exchanged through the system remains the property of and under the legal control of the USSS; and
- Each individual is responsible for their own compliance in collecting, maintaining, and sharing information under the Privacy Act and any applicable regulations.

Privacy Risk: There is a privacy risk that exams conducted for employment purposes may be used for a law enforcement purpose.

Mitigation: To mitigate this risk, policies and procedures are in place to ensure that data is used in accordance with each respective authorized uses for information contained FSD Polygraph system. All information will be used in conformity with DHS/USSS-001 (Criminal Investigative Information System, 76 FR 49497) System of Records Notice (SORN) and consistent with all existing MOU/MOAs.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Names and identifiers of individuals who are administered a polygraph examination, as well as exam results and other information on the SF-86, may be retained by USSS.

3.2 How long is information retained?

Existing retention schedules, established and/or approved by the National Archives and Records Administration (NARA), may cover periods as short as two years for individuals examined by the Secret Service in relation to applicant processing or indefinitely with investigations that involve crimes in which there is no statute of limitations (e.g., murder). Information which is collected that does not become part of an investigative case file will be destroyed/deleted after two years when it is collected as part of an applicant investigation; after five years if it is performed for other government agencies; or when no longer needed for administrative, legal or audit purposes; whichever is later.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

No, USSS is currently working towards the approval of disposition schedules by the Secret Service Chief Records Officer and NARA.

However, various approved record schedules exist which describe and define retention periods for polygraph records (e.g., N1-87-86-2, "Polygraph Examinations Maintained by the Forensic Services Division.") These approved schedules will serve as the basis for a new comprehensive schedule specific to the FSD Polygraph System, which is being developed for approval by the component records officer and by NARA.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: There is a risk that polygraph data could be maintained for a period longer than necessary to achieve agency's mission.

Mitigation: Although there is always risk inherent in retaining personal data for any length of time, the polygraph data retention periods based on case type identified in the NARA schedules are consistent with the concept of retaining personal data only for as long as necessary to support the agency's mission. Further, the system is available only to authorized Secret Service personnel, and law enforcement agencies, and must be used in conformance with applicable laws and regulations.

The Secret Service retains the information no longer than is useful or appropriate for carrying out the information dissemination, collaboration, or investigation purposes for which it was originally collected. Information which is collected that becomes part of an investigative case file will be retained for a period which corresponds to the specific case type developed (e.g., judicial, non-judicial, non-criminal, etc.).

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Only criminal-related exam information may be shared with any eligible DHS component agencies with law enforcement authority to the extent required to enable authorized officials to complete their functions and responsibilities. Authorized officials may include those with a need-to-know do so that they may investigate potential criminal activity.

4.2 How is the information transmitted or disclosed?

Criminal database information is transmitted to law enforcement or court-mandated agencies verbally. If USSS retains an actual copy of the examination results report, with consultation from Office of Chief Counsel, a paper copy of the report would be faxed. For applicants, reports are released only via a USSS vetted and approved FOIA request.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: Privacy risks associated with internal sharing of the data is unauthorized access to, or disclosure of, PII contained in the system.

Mitigation: To mitigate this risk, access to the system is limited to authorized personnel with a need to know. DHS policies and procedures are in place to limit the use of and access to data in the system to the purposes for which it was collected. All authorized users must log on using a two-factor authentication. Further, local field offices verify the status and ongoing need of the investigation. If information is needed on an exam that a polygraph examiner did directly for a law enforcement agency, then the examiner would verify the recipient's need for this information.

All DHS employees and contractors are required to follow DHS Management Directive (MD) Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, May 11, 2004. This guidance controls the manner in which DHS employees and contractors must handle Sensitive but Unclassified/For Official Use Only Information. All employees and contractors are required to follow Rules of Behavior contained in the DHS Sensitive Systems Handbook. Additionally, all DHS employees are required to take annual computer security training, which includes training on appropriate use of sensitive data and proper security measures.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which included federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared and for what purpose?

USSS administers exams to subjects of allegations to assist local and state law enforcement as well as some federal agencies. Polygraphs given to support state and local law enforcement are generated from their offices. They will directly contact either the local USSS polygraph examiner or the local field office and request assistance in a particular case. Exams conducted at the request of state and local law enforcement agencies are generally conducted to provide forensic and investigative support in investigations involving missing or exploited

children in accordance with 18 U.S.C. § 3056(f). Some exams may be conducted on subjects in state and local law enforcement investigations involving major felonies.

With respect to federal agency requests for polygraph support, there is a Memorandum of Understanding between USSS and DHS/OIG and OIG requests are vetted through the USSS Office of Professional Responsibility and the USSS Inspection Division for authorization. For any exams run for a federal agency, the exam will not be run in internal affairs/administrative cases. USSS polygraph examinations for federal agencies, other than OIGs, are quite infrequent and are conducted only for those agencies that do not have existing polygraph programs. As such, they are conducted in the absence of any MOU/MOA's using the same approval process as for OIG.

Only criminal-related polygraph examination information is shared with accredited law enforcement agencies outside of DHS on a need to know basis to support criminal investigations and assignments by the Secret Service. Information may be shared in accordance with the purposes and routine uses specified in the Secret Service's System of Records Notice DHS/USSS-001 (Criminal Investigative Information System, 76 FR 49497) in support of the USSS investigative mission.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing of PII outside the department is compatible with the original collection. The system was developed for the purpose of sharing a limited amount of information to law enforcement agencies with investigative responsibilities.

As an investigative information system owned by the Secret Service, the database is covered by the DHS/USSS-001 (Criminal Investigative Information System, 76 FR 49497) System of Records Notice (SORN) which specifies how the information be may used. Also, all Secret Service employees and contractors are trained on the appropriate use of PII. The sharing of information between the Secret Service and participating agencies is covered by and consistent with the routine uses contained in the DHS/USSS-001 SORN.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The criminal examination data is shared between the Secret Service and other participating accredited law enforcement agencies. The Secret Service bears responsibility for the security of the portal and transmission of the data to participating agencies. Any information shared with organizations outside the Secret Service is required to be appropriately secured

pursuant to the Office of Management and Budget Memorandums 06-15, Safeguarding Personally Identifiable Information, and 06-16, Protection of Sensitive Agency Information.

5.4 Privacy Impact Analysis: Considering the external sharing, explain the privacy risks identified and how they were mitigated?

Privacy Risk: The primary privacy risk associated with external sharing is the sharing of data for purposes that are not compatible with the original purpose of the collection.

Mitigation: This risk is mitigated by limiting access to the database by only permanently assigned QC polygraph examiners within the Secret Service members. When logging on to the database, users must also acknowledge they are accessing a government information system and agree to adhere to rules and regulations concerning information sharing and confidentiality.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

In all instances the individual has consented to the use of the polygraph. A Statement of Consent is presented to the examinee and must be voluntarily executed. At any time during the polygraph, the examinee may opt to terminate the examination.

Further, the System of Records Notices DHS/USSS-001 (Criminal Investigative Information System, 76 FR 49497) and DHS/USSS-003 (Non-Criminal Investigative Information System, 76 FR 66937) provide notice regarding the collection of information and the routine uses associated with the collection of the information. The final rule for the systems of records officially exempts the systems from portions of the Privacy Act.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

All polygraph examinations are voluntary. Individuals must sign a Statement of Consent prior to any exam being administered. Those applying for USSS employment may decline the polygraph examination or may depart the examination at any point; however, by doing so, they forfeit further consideration for employment as the examination is required to determine eligibility.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals do not have the right to consent to particular uses of the information.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided to individuals at the time of examination as information is collected directly through the interview of the examinee, and all examinees must sign a Statement of Consent prior to the exam being administered. Further, notice is provided herein and through DHS/USSS-001 and DHS/USSS-003 SORNs.

Section 7.0 Access, Redress and Correction

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

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/USSS-001 SORN.

7.2 What are the procedures for correcting inaccurate or erroneous information?

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

7.3 How are individuals notified of the procedures for correcting their information?

The mechanism for requesting correction of information is specified in the System of Records Notices DHS/USSS-001 (Criminal Investigative Information System of Records Notice 76 FR 49497) and DHS/USSS-003 (Non-Criminal Investigative Information System of Records Notice, 76 FR 66937).

7.4 If no formal redress is provided, what alternatives are available to the individual?

See Section 7.3.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated?

Privacy Risk: There is a privacy risk of inaccuracies in polygraph exam results.

Mitigation: All USSS examiners are undergo rigorous training and testing prior to being deemed

qualified to administer polygraph examinations. Nonetheless should examinees believe that the results of examination are erroneous, redress is available through written request to the Secret Service Freedom of Information Officer as described above; however, providing individual access and/or correction of the records may be limited for law enforcement reasons as expressly permitted by the Privacy Act.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

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.

8.2 Will Department contractors have access to the system?

No. All USSS users of the polygraph database are USSS employees.

8.3 Describe what privacy training is provided to users to either generally or specifically relevant to the program or system?

All USSS employees 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.

8.4 Has Certification and Accreditation been completed for the system or systems supporting the program?

The certification and accreditation was completed on August 9, 2010, and expires on August 9, 2013.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

All Department information systems are audited regularly to ensure appropriate use and access to information. Specifically related to this system, application access is mediated through a two-tier identification and authentication process. End users must successfully gain access to the USSS net before they can access the polygraph database application. USSS.net access is restricted to a population of known user IDs that are generated when the USSS.net account is issued and manually entered into the database users table by the system administrator. Any changes to the hardware or software configuration are subject to review and approval by the

Secret Service Configuration Control Board process to ensure integrity of the application.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: The risk of unauthorized access exists with any information technology system.

Mitigation: Access to the polygraph database is restricted to QC examiners within the Polygraph Operations Branch. Information shared via this database is limited to personal identifiers and test outcomes.

Access Control

- Access/control is restricted to users with a valid userid and password. In addition to the userid and password, the user must have an assigned certificate installed on the user's workstation for access through USSS.NET. If the user is on the USSS Network, access is granted via the USSS network active directory account.
- Session timeouts, user selectable from 10 minutes to 4 hours with 30 minutes the system default.
- The account is locked after 3 consecutive incorrect sign on attempts.

Auditing

- All accounts are audited by the USSS Polygraph system administrator.
- The audit trail provides a timestamp and userid.
- The information is recorded into the database for each log on/off attempted.
- The contents of audit logs are protected from unauthorized access, modification, and/or deletion. Administrator privilege is required for access to audit logs.

Section 9.0 Technology

9.1 What type of project is the program or system?

The polygraph database system is an information-collection tool.

9.2 What stage of development is the system in and what project development lifecycle was used?

The system is in the operations and maintenance lifecycle phase.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The project does not employ technology that could raise privacy concerns.

Responsible Official

A. T. Smith
Assistant Director – Office of Investigations
United States Secret Service
Department of Homeland Security
Office: 202-406-5716

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security