Privacy Impact Assessment
for the

Suspicious Activity Reports Project

November 21, 2008

Contact Point
Wesley Moy
Deputy Director
National Operations Center
Department of Homeland Security
Office of Operations Coordination and Planning
(202)-282-8187

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Office of Operations Coordination and Planning (OPS), in cooperation with the Science and Technology Directorate (S&T) is publishing this PIA to reflect a planned research project regarding Suspicious Activity Reports (SARs). The Operations Coordination and Planning Directorate will host a stand-alone system designed to analyze Suspicious Activity Report data taken from several Department of Homeland Security (DHS) components. OPS has conducted this PIA because SARs occasionally contain personally identifiable information (PII) and because it is physically hosting the project in addition to contributing SARS data.

Overview

Background

Several components within DHS collect and use Suspicious Activity Reports (SARs) in the execution of their mission and operational duties. SARs are defined by the Program Manager – Information Sharing Environment (PM-ISE) as "observed behavior that may be indicative of intelligence gathering or pre-operational planning, related to terrorism, criminal, or other illicit intention."[1] All SARs are centered on activities, meaning that an event or action has occurred that has aroused some degree of suspicion.

DHS components collect SARs which are stored and used as they are received during the course of daily operations in law enforcement, maritime, intelligence, and other sectors in which DHS has a presence. While each DHS component will collect and analyze SARs data as it has done in the past, until recently DHS has not had a unified method to analyze SARs data across DHS components. This means that SARs data collected by one DHS component was analyzed under parameters significant to, for example, the border and customs sector, and not necessarily for immigration or other intelligence purposes.

As part of their statutory duties, the Office of Operations Coordination and Planning (OPS) and the Science and Technology (S&T) Directorates are hosting a research project designed to determine how best to analyze component SARs data under a single set of DHS-wide tools and parameters. The two primary goals of the project are 1) to make available useful SAR data from across DHS and 2) determine which technology tools are most useful in analyzing SARs. This will allow Ops, S&T, and other DHS components to determine whether some SAR data collected by individual components, which may not on its face have a nexus to terrorism, may in fact prove to have a nexus to terrorism, criminal, or other illicit intention when coupled with other components' information.

Project Objective

SARS data is used at each DHS component in order to analyze information as it pertains to the respective component; However, information in a SAR which is not valuable to a component within a certain sector may in fact be valuable to a component in another sector. This project is designed to bridge

[1] PM-ISE Initial Privacy and Civil Liberties Analysis of SAR Functional Standard. The Information Sharing Environment (PM-ISE), as established as part of the National Strategy for Information Sharing (NSIS), helps to coordinate comprehensive efforts across local, state, tribal, and federal communities to share terrorism-related information, which includes terrorism-related SARs.
http://www.ise.gov/docs/sar/ISE_SAR_Initial_Privacy_and_Civil_Liberties_Analysis.pdf

that gap with the objective of how to best establish a single DHS protocol for the collection and analysis of SARs data. Once the project concludes, each component contributor will determine the relative value of the project to the component, and convene with other components at the Project Steering Committee to determine the value of the project to the Department.

Project Structure

In order to determine the cross-component relevance of SARs data, it is necessary to make the SARS data of one or more components available to other components. The project's plan is to create a single, off-line, stand-alone system which will house SARs data from various DHS components. Specifically this system will consist of two computer terminals and three processing and storage servers. The computers and processors used will not be connected to any network at DHS or any other component.

OPS will provide the physical space for the computers and processing servers. The computers will be stored in a secure room at the OPS facility which will be restricted to authorized entry only. Data copied to the system will remain static and will not be updated after it is initially uploaded.

Research and Analysis

S&T, through contracted software vendors and research laboratories, will provide applications and tools with which to search the data. These tools and applications will be installed on the computer terminals and servers and be available for use by any participating component user.

At the outset of the project, several types of analysis will be available to component users. DHS component contributors to this project are not necessarily aware which analytical toolsets will be valuable and which will not in relation to the analysis of SARs data. Because SARs data is related to activity, not individuals, it is foreseen that most tools will be centered on determining trends or links between specific types of activities discovered at certain types of locations. PII will be searchable in conjunction with non-PII activity based information.

Data Sources

SARs data from contributing components will be used to populate the computers. The data will be transferred via physical copy, specifically CD-Rom or external storage device. This SARs data will be static; it will not be updated by the contributing component through the course of this project. Data sources are detailed in Sections 2, 5, and 6 of this PIA.

Privacy Controls

All SARs imported into the system which contain PII will be tagged as containing PII. The significance of the tag is that any document retrieved in a search that contains PII will include a banner indicating that the document contains PII, and any information handling protocols required by the contributor's component must be followed. In the future, OPS, S&T and their partners plan to implement a PII masking function which will automatically mask PII in a retrieved document. PII will only be unmasked once the user affirmatively acknowledges and proves his/her need to know the information. This will ensure that the PII accessed by users is limited. Using this method, the pilot project and future implementations of this technology can meet the information handling requirements of the Intelligence and Law Enforcement Communities, specifically Executive Order 12333 and 28 CFR Part 23. Additionally, analysts participating in this pilot are required to complete Protected Critical Infrastructure Information (PCII) training to ensure the proper handling and privacy protocols for viewing data that potentially

contains PCII. Anyone viewing this data will be trained and have a signed Non-Disclosure Agreement on file.

Once the testing phase is complete, each component will review the effectiveness and value of the testing as it pertains to their mission. OPS will dismantle the system and delete any data stored on the self-contained system.

Typical Transaction

A participating component's analyst will arrive at the OPS facility seeking to analyze data in the research project. The analyst must first appropriately access the OPS building, and then separately access the room housing the SARs project terminals. Once the analyst is at the terminal, they must log into the system with a unique credential and identification.

After logging onto the system, the analyst (user) will be presented with an icon to launch Café. Café is a windows based, Java-script application. Café serves as the launching point for other COTS and custom developed decision analytics tools. Within Café, the user will be presented with a file directory tree representing the set of data in the system available for analysis. The user can then select one or more files from the file directory tree to be used within a specific decision analytics tool. Depending on the tool selected, the user will generally see a screen that depicts the visualization of the selected data within the specific tool.

Future

No determination has been made whether OPS will be the ultimate owner of a DHS-wide SARs system, or whether such a system will exist. Each component will review the relative value of this research project and report back to S&T on whether a formal DHS SARs system would be of value to their mission needs.

DHS is aware of the parallel PM-ISE's SAR Initiative.[2] As the DHS SAR Project develops, DHS and its components will continue to be informed by the PM-ISE's SAR Initiative and its goals. DHS's use of SARs is consistent with its membership in the ISE and its related SAR initiative.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

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

Data uploaded into the system will be tagged as having come from a particular system of records source. Information will not differ from the original collection at the component agency, which is activity data, i.e., a certain suspicious event occurred at a certain place. PII may enter the system as it pertains to a suspicious event, e.g., a suspicious person committed a suspicious act. PII may be limited to basic

[2] PM-ISE Initial Privacy and Civil Liberties Analysis of SAR Functional Standard.

descriptive data (hair color, height, sex/gender, etc) or specifically identifying PII (name, date of birth, etc).

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

The sources of any PII are the initial systems of records of the components, specifically at the Operations Directorate, Transportation Security Administration, and the National Protection and Programs Directorate. This PIA will be updated once new components begin participation.

It is possible that some of the PII within a SAR is provided by individuals themselves as gathered by the original collector, but that is not necessarily known or knowable by OPS or S&T for this project.

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

SARs are initially collected and generated as part of the ongoing mission operations of the participating components. Any suspicious activity occurring on the U.S. border or in the maritime, transportation, infrastructure, key resources, immigration, and other sectors may result in the formal submission of a SARs. SAR data supports the daily operations of each DHS component and is collected because of its relative analytical value to those operations.

By combining certain SAR data sets, DHS will be better able to interpret SAR data and its potential value to combating terrorism and protecting the United States.

1.4 How is the information collected?

Information in this project is collected in electronic form (hard disk, CD) from the components themselves. SAR data is originally collected by observation, interaction, and other daily law enforcement and intelligence activities.

1.5 How will the information be checked for accuracy?

Generally, participants will not check the information for accuracy. Information may be cross referenced with other component SARs data, or verified through systems of records within an individual component. SARs data is taken "as is" for analysis purposes only. Any action taken on based on any SARS data in this project would be properly vetted and researched through a component's appropriate channels.

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

The Homeland Security Act of 2002 as codified within the United States Code at 6 U.S.C. § 121(d)(1); 6 U.S.C. § 121(d)(4); 6 U.S.C. § 121(d)(11); 6 U.S.C. § 121(d)(12)(A); 6 U.S.C. § 121(d)(15); and 6 U.S.C. § 121(d)(17) provide DHS and the NOC with authority to collect the

information. Participant component system of records notices cite the authority for the original collection of the SARs data.

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

The privacy risks presented regarding scope are that more information will be collected or available than was previously accessible. This is partly the intent of the program: to provide more access to SARs data that certain components have not previously shared. This is mitigated by the fact that DHS is concerned with any SAR data that may have a relationship to one of DHS's missions, including but not limited to infrastructure protection, border and customs enforcement, and transportation security. DHS components receive SAR data from law enforcement agencies at the Federal, State, and local level; however, such SAR data must relate to the mission of the component of DHS who collected the information, and for use in this project, could have a nexus to terrorism.

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 all the uses of information.

Participating DHS components will use the system to analyze SARs information as it is collected across several DHS systems of records. Specific uses will be to determine any links or unforeseen associations between SARs data collected by DHS agencies in the course of their mission duties.

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

S&T contractors and laboratory partners will provide analytical tools and applications for this testing phase. DHS component participants are not necessarily aware of what value certain types of toolsets will or will not be important in relation to the analysis of SARs data. This project is designed to determine which types of tools are best able to analyze SARs information. As stated above, most SARs data is related to activity, not individuals. It is foreseen that most tools will be centered on determining trends or links between specific types of activities discovered at certain types of locations. PII will be searchable in conjunction with non-PII activity based information, e.g., determining if a person submits the same false name at different facilities or locations.

One of the major purposes of this project is to determine which analytical tools are most beneficial to DHS and DHS components when analyzing SARs data. This could involve link analysis, basic Boolean searches, relationship searches, or any other type of search that is conceivably beneficial to a particular analyst's needs. As the project proceeds, the most valuable tools will likely surface, thereby informing DHS and participating components which analytical tools are most helpful in SARs analysis.

A secondary benefit to the project is to determine whether SARs data is valuable in the national security environment, or more specifically, whether some types of SARs prove more beneficial than other types of SARs. This project will better enable DHS to make determinations about the value of certain types of SARs data.

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

The system does not use commercial or publicly available data. All SARs data is based on observation, interaction, or other authorized law enforcement or intelligence activity.

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.

All information containing PII that is uploaded into the system will be tagged as containing PII and belonging to a certain component system of records. This tagging enables the system's software to tag each document as containing PII and place a banner at the top of each document retrieved stating that the document contains PII and should be handled appropriately.

For future implementations, in order to comply with Executive Order 12333 and 28 CFR Part 23 regarding minimization of US Person information, all PII will be masked at the initial retrieval of a PII tagged document. The document's PII may be unmasked by a user once they acknowledge that they have the rights and "need to know" the PII in order to fulfill the mission-related research.

If a participating component finds actionable information in the project, coordination for action and sharing of information will be made between the component seeking to use the SARs data and the originator of the SARs data. All sharing will comport with section (b)(1) of the Privacy Act and applicable system of records notices (SORN).

These controls ensure that the users of the system undertake affirmative steps to acknowledge the appropriate access and use of the information.

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?

All data provided by SARs participant agencies will be retained in their respective system of records in accordance with the System of Records Notices (SORNs) published for each information collection (see Section 6 "Notice" below). There are no official "results" of the project; the only result of the project is a qualitative analysis by participating components on the relative value of SARs and the analytical tools. All data used in the project will be purged from the system.

3.2 How long is information retained?

Data stored on the terminal housed by OPS will be stored in accordance with the records schedule formally submitted to NARA by the respective source system components.

After the project has been completed and it has been determined by the Program Manager that the system should be dismantled, all of the system data (stored on the servers or on external media) will be destroyed. Any output required to support the proof of concept will remain in the lab until it is no longer required or up to a period of one (1) year after the conclusion of this project. Any records derived from this project will be stored in accordance with the HSIN DB records schedule (NARA # N1-563-08-19 and /or GRS 20, item 2a, 2b, 5, 6, & 7, which states generally that master file/data must be deleted after 20 years and reporting information may be deleted when the record is no longer needed for administrative, legal, audit, or other operational purposes)

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

Each component source system is responsible for its own records schedule submission to NARA.

NOC Homeland Security Information Network (HSIN) Database (Homeland Security Operations Center Database, April 18, 2005, 70 FR 20156): HSOC personnel plan to request records disposition schedules and coordination of those schedules with the National Archives and Records Administration (NARA) for ten years from the time of inclusion in the HSIN Database. Not all records will remain active during this time; rather, it is anticipated that the HSIN Database will maintain both active and inactive records. HSIN users will be required to change the status of their submissions from active to inactive if an incident is determined to have no nexus to terrorism. The system will provide HSIN users with reminders for active reports that have not been resolved after a certain period of time.

National Infrastructure Coordinating Center (NICC) INSight (Homeland Security Operations Center Database, April 18, 2005, 70 FR 20156): Same as above.

FAMS Tactical Info Sharing System / Surveillance Detection Reports Database (Transportation Security Enforcement Record System DHS/TSA 001, December 10, 2004, 69 FR 71828): National Archives and Records Administration approval is pending for the records in this system. Once approved, paper records and information stored on electronic storage media are to be maintained within TSA for five years and then forwarded to Federal Records Center. Records are destroyed after ten years.

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

A risk is posed by the potential complexity of the retention schedules for each of the source systems. Because each source system has a different retention schedule, sorting out which data would need to be deleted at which time could prove difficult. However, this risk is completely mitigated by three

factors. First, all data in this project is data copied from the original source; these are not the original records and may be destroyed at any time as long as that time is not longer than the approved schedule. Second, and more importantly, any data used in this project will be returned to the source system and deleted from the pilot project system at the close of the project. Lastly, the length of this project will be shorter than the shortest retention schedule of the source systems.

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?

The primary purpose of this initiative is to share and analyze data across DHS components.

Should any data discovered during testing be apparently actionable by DHS or its components, such data would be taken back to the component responsible for action or dissemination. All information shared between DHS components, is shared within the Department pursuant to the Privacy Act § (b)(1).

4.2 How is the information transmitted or disclosed?

Information will be transmitted to the SARs project terminals and servers via hard copy, most likely encrypted cd-rom or other external storage device. Any actionable information (information that must be acted upon by a component or components immediately) will be transmitted via the same method. Any physical media that leaves the facility must first be approved by the ISSO. Physical media will be taken to the appropriate component for action.

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.

The primary purpose of this project is to facilitate internal sharing through the identification of common resources and needs and streamlining of information analysis processes across the Department. Risks associated with internal sharing would be the inappropriate sharing of SARs data, and the inappropriate use of SARs data outside of this project. These risks are mitigated by the fact that DHS is considered one agency and any information sharing within the agency may occur as long as a need to know exists with the recipient agency. Each participant in this project is willingly providing data and agree to the terms of use of the system, its data, and any appropriate uses.

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 includes 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?

No data from this project will be disclosed outside of DHS unless determined to be an actionable pursuant to DHS and the component's statutory responsibilities. Any sharing would be done pursuant to the source system's SORN.

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.

Although not anticipated, should mission need require it, any sharing outside the Department would conform to the following participant SORNs:

NOC Homeland Security Information Network (HSIN) Database (Homeland Security Operations Center Database, April 18, 2005, 70 FR 20156)

National Infrastructure Coordinating Center (NICC) INSight (Homeland Security Operations Center Database, April 18, 2005, 70 FR 20156)

FAMS Tactical Info Sharing System / Surveillance Detection Reports Database (Transportation Security Enforcement Record System DHS/TSA 001, December 10, 2004, 69 FR 71828)

As other DHS components begin to participate in this project, their source SORN will be updated into this document.

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

Should actionable information be discovered in during this research project, information will be shared according to the requirements of any SORN associated with the outgoing data.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

A risk exists that any information used or produced from this project may be inappropriately shared to an external agency. Because each contributing agency's data is simply a copy, and the original SARs data is still within its original system of records, each participant component may share its own SARs data with any agency it deems necessary as long as any legal, policy, and procedural requirements are met to complete the sharing.

Any data produced by this project and stored by OPS in the HSIN Database will be shared in compliance with OPS' authorities, protocols and the HSOC SORN.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

This PIA serves as notice of the SARS Research Project. Notice of the initial collection of SARS data is provided by individual components through, at a minimum, the SORNs cited below.

NOC Homeland Security Information Network (HSIN) Database (Homeland Security Operations Center Database, April 18, 2005, 70 FR 20156)[3]

National Infrastructure Coordinating Center (NICC) INSight (Homeland Security Operations Center Database, April 18, 2005, 70 FR 20156)[4]

FAMS Tactical Info Sharing System / Surveillance Detection Reports Database (Transportation Security Enforcement Record System DHS/TSA 001, December 10, 2004, 69 FR 71828)

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

The majority of SARs data does not involve the collection of PII. Any PII within a SARs is collected appropriately during the course of a participating agency's operations. Should an individual be involved with a suspicious event, his or her information is directly relevant to the incident at hand. As part of that suspicious incident, any information provided by the individual will be included in the SARs if it is relevant.

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

PII contained within a SAR is used in accordance with the SORN for the SARs data as well as any other mission requirements placed on the participating component.

[3] http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-7704.htm

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.

Formal notice of this project is provided by this PIA. Any notice provided at the point of collection is the responsibility of the respective participating components. At a minimum, the SORNs cited above provide notice that components within DHS collect and use SARs data for their mission needs. Appropriate notice may have been provided at the time of collection, however, during law enforcement and intelligence activities such notice be counter-productive or simply impossible in the context of certain operations.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Any individual access or information requests should be directed at the contacts provided in the SORNs for each source system (see Notice above) and/or to the following FOIA contacts:

Director for Operations Coordination

U.S. Department of Homeland Security
Washington, D.C. 20528
FOIA Officer/Requester Service Center Contact: Michael Page
Phone: 202-282-8743
Fax: 202-282-9069
E-mail: FOIAOPS@DHS.GOV

Under Secretary for Science & Technology

U.S. Department of Homeland Security
Washington, D.C. 20528
FOIA Officer/Requester Service Center Contact: Miles Wiley
Phone: 202-254-6819
Fax: 202-254-6178
E-mail: stfoia@dhs.gov

Under Secretary for National Protection and Programs

U.S. Department of Homeland Security
Washington, D.C. 20528
FOIA Requester Service Center Contact: Gayle Worthy
Phone: 202-282-9021
Fax: 202-447-3250
E-mail: NPPD.FOIA@dhs.gov

Transportation Security Administration

Freedom of Information Act Office, TSA-20
601 S. 12th Street
11th Floor, East Tower
Arlington, VA 22202-4220
FOIA Officer: Kevin J. Janet
FOIA Requester Service Center Contact: Deborah Snowden
Phone: 1-866-FOIA-TSA or 571-227-2300
Fax: 571-227-1406
E-mail: foia.tsa@dhs.gov

.

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

For this project, all data will remain static until the end of the project. No data will be updated. As for source systems, SARs data is raw situational and incident data. It is not corrected or updated in any way. If SARs data is incorporated into a formal report by a component it may be verified and potentially updated, but SAR data is raw and unfinished information.

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

The SORNs for each source system provide information on how to correct information.

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

Formal redress is provided through the SORNs for each system as well as through FOIA.

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

Formal redress is provided, at a minimum, by the Privacy Act and FOIA processes at DHS and its components. The processes are outlined in the SORNs for each participating component, and those SORNs are cited in Section 6.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

System access will be restricted to the performing contractors and authorized Federal personnel directly involved in the pilot project. Contractors will be required to sign in for lab access and log access to the system. An access control roster will be kept for access to the space and the system will require login (passwords/usernames).

8.2 Will Department contractors have access to the system?

Yes.

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

Annual privacy and security training are provided to each DHS component employee. Any training specific to SARS data is the responsibility of the respective participating agencies.

Prior to incorporation of any component's data, the potential user group from the component will receive a demonstration and training on how the system and interface will work, and how the security and privacy controls will work, among other types of training.

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

No. Since this is not a production system, nor will it be connected to any production systems, certification & accreditation is not required.

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

Each user that logs into the system will do so under a named account with a username and password. Accounts will not be shared between multiple users. Password protection procedures have been instituted to minimize break-in attempts. These include 1) minimum password complexity rules, 2) password rotation every ninety days, 3) account lockout after four invalid login attempts. All system level actions performed by a user will be audited and logged to a file. The log files will remain persistent on the machine and are accessible only to system administrators. Anti-virus software will be installed and running as system processes for all windows machines. The virus definition files will be updated weekly through physical media. PII data will be tagged and masked and analysts will be properly trained on handling PCII. These and additional safeguarding requirements are outlined in a separate document (SARS Pilot Lab Standard Operating Procedures). Non-Disclosure Agreements have been signed as well.

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?

One of the primary reasons OPS is hosting the physical computer terminal is because OPS can provide a secure facility and space to house the system. Each individual authorized through DHS security procedures to access the OPS building must also be authorized to access the room housing the computer terminal. Once the individual user reaches the computer terminal he/she will be required to enter his or her specific log-in information in order to access the terminal and use the testing data.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The SARS project is designed purely for research through a stand-alone, non-networked system.

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

The SARS project is nearing its final stages for testing SARS analytical tools across DHS components.

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

Yes. A privacy concern presented by a project of this breadth is the commingling of data from separate systems of records. To mitigate this risk, data imported into the system will be tagged as having come from a particular source system of records. This ensures that for any data retrieved in a search, the user knows which system of records the information came from and how it is best handled.

Another privacy risk is presented by individuals not being aware of whom to direct information requests to regarding this project or SARS data in general. Individual SORNs have been published for each source system, and they are cited in this document. This ensures that any individual requesting information on him or herself can reach the appropriate person within each DHS component.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security