PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**SAFETY Act Management System**		
Component:	Science and Technology (S&T)	**Office or Program:**	Office of Public-Private Partnerships – SAFETY Act Office
Xacta FISMA Name (if applicable):	**SAFETY Act Management System**	**Xacta FISMA Number (if applicable):**	**SAT-05799-MAJ-05799**
Type of Project or Program:	**IT System**	**Project or program status:**	**Operational**
Date first developed:	**December 14, 2006**	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	**October 9, 2012**	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable)	**In progress**	**ATO expiration date (if applicable):**	**June 30, 2016**

PROJECT OR PROGRAM MANAGER

Name:	**Bruce Davidson**		
Office:	**Office of Public-Private Partnerships**	**Title:**	Director, Office of the SAFETY Act Implementation
Phone:	**202-254-5792**	**Email:**	Bruce.Davidson@hq.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**Timothy Schaad**		
Phone:	**703-674-2773**	**Email:**	Timothy.schaad@associates.hq.dhs.gov

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Renewal PTA
This PTA renewal is being submitted for security authorization renewal purposes. No new PII is being collected, used, or shared. SAFETY Act is a congressionally mandated program (6 USC 101) administered by the Department of Homeland Security (DHS) that provides important legal liability protections for providers of qualified anti-terrorism technologies – both products and services. The goal of the SAFETY Act is to encourage the development and deployment of new and innovative anti-terrorism products and services by providing liability protections. Companies seeking legal liability protection for their offerings submit applications to DHS, which are then carefully evaluated and approved on a case-by-case basis, and subject to stringent protections to safeguard the applicants and their technologies. As both applicants and evaluators are geographically dispersed, DHS requires an automated, reliable, and secure mechanism that enables industry to submit applications, supports information sharing and collaboration among evaluators, and allows the official results of the evaluation to be communicated to the applicants. The SAFETY Act Management System (SAMS) is the technical solution built to manage the end-to-end application submittal and evaluation process. SAMS comprises two major subcomponents: 1) a public-facing website that allows applicants to submit and track their applications, and 2) a back-end business process management application that supports the evaluation process within an access-controlled and auditable environment.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	□ Closed Circuit Television (CCTV) □ Social Media □ Web portal[1] (e.g., SharePoint) ☒ Contact Lists □ None of these

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☒ DHS employees/contractors (list components): ☒ Contractors working on behalf of DHS ☐ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?
All users: • Username & Password • First Name & Last Name • Business Address • Business Phone/fax number(s) • Business Email address

4(a) Does the project, program, or system retrieve information by personal identifier?	☐ No. Please continue to next question. ☒ Yes. If yes, please list all personal identifiers used: Authorized users can retrieve user information by name, business, or SAFETY Act Application number
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item. Please describe applicable information sharing governance in place:
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: All personnel supporting SAMS receive tailored role-based training, including Administrators, Subject matter Experts (SMEs), and staff.
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures	☐ No. What steps will be taken to develop and maintain the accounting:

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

of PII to individuals who have requested access to their PII?	☒ Yes. In what format is the accounting maintained: An Excel spreadsheet is generated and stored in the SAMS Program's document repository.
9. Is there a FIPS 199 determination?[4]	□ Unknown. □ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: □ Low □ Moderate ☒ High □ Undefined Integrity: □ Low ☒ Moderate □ High □ Undefined Availability: ☒ Low □ Moderate □ High □ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Christopher S. Lee**
Date submitted to Component Privacy Office:	**June 6, 2016**
Date submitted to DHS Privacy Office:	June 7, 2016

Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*
The SAFETY Act system is currently covered under the General Contact Lists PIA and the S&T-001 - Research, Development, Test, and Evaluation Records SORN. I recommend continued coverage under these privacy compliance documents.

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Gina Mostafaie
PCTS Workflow Number:	1125917
Date approved by DHS Privacy Office:	June 23, 2016
PTA Expiration Date	June 23, 2019

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. ☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	System covered by existing PIA If covered by existing PIA, please list: DHS/ALL/PIA-015 - DHS Web Portals
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/S&T-001 - Research, Development, Test, and Evaluation Records DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS)

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

S&T has submitted the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) for its three-year recertification. The SAFETY Act is part of DHS Act of 2002, Public Law 107-296, which makes it permissible to improve U.S. Government anti-terrorism readiness. The SAFETY Act is implemented by the Office of SAFETY Act Implementation (OSAI) and reports to director of the Office of Public-Private Partnerships within the R&D Partnerships Group at the DHS S&T. The reason for this Act is to confirm that accountability concerns do not prevent producers from developing anti-terrorism technology, thus saving lives. The SAFETY Act pertains to a breadth of technologies that includes products, services, software and other forms of intellectual properties (e.g., sensors, detection systems, cyber security technologies, etc.).

The DHS Privacy Office finds the SAFETY Act to be a privacy-sensitive system because this IT system collects, uses, maintains and disseminates personally identifiable information (PII) from the members of the public, DHS employees, and contractors. The collected PII from users include full name; username; password; and business address, phone and fax number; and email address.

The DHS Privacy Office finds DHS/ALL/PIA-015 - DHS Web Portals provides coverage for this IT system because this is a web portal and this PIA was written to provide coverage for PII collected from the members of the public by DHS in order to document informational and collaboration-based portals in operations at DHS and its components. These online portals allows limited PII about individuals who are members of the portals or seeking to gain access to portal.

The DHS Privacy Office finds that DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS), and DHS/S&T-001 - Research, Development, Test, and Evaluation Records SORNs apply because the SAFETY Act retrieves PII by unique identifier (name, business, or application number).

The purpose of the DHS/ALL-004 – GITAARS is to provide authorized individuals access to and allow interaction with DHS information technology resources.

The purpose of the DHS/S&T-001 - Research, Development, Test, and Evaluation Records SORN is to “furthering S&T's mission to push innovation and development, and the use of high technology in support of homeland security. The purposes of the records are to: Understand the motivations and behaviors of terrorists, individuals that engage in violent or criminal activities, terrorist groups, and groups that engage in violent or criminal activities, terrorist groups, and groups that engage in violent or criminal activities.”