Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

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:	**Sexual Abuse and Assault Prevention and Intervention (SAAPI) Case Management**		
Component:	Immigration and Customs Enforcement (ICE)	**Office or Program:**	Enforcement and Removal Operations, Custody Management (ERO/CMD)
Xacta FISMA Name (if applicable):	**N/A**	**Xacta FISMA Number (if applicable):**	**N/A**
Type of Project or Program:	**IT System**	**Project or program status:**	**Operational**
Date first developed:	**February 19, 2015**	**Pilot launch date:**	**N/A**
Date of last PTA update	**February 19, 2015**	**Pilot end date:**	**N/A**
ATO Status (if applicable)	Choose an item.	**ATO expiration date (if applicable):**	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	**Patricia Reiser**		
Office:	**ERO/CMD/Detention, Evaluation and Analysis**	**Title:**	**Detention and Deportation Officer**
Phone:	**610-587-9123**	**Email:**	Patricia.Reiser@ice.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**Andrew Robeson**		
Phone:	**202-732-7073**	**Email:**	Andrew.j.robeson@associates.dhs.gov

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Renewal PTA

This PTA Renewal is being submitted to complete the mandatory three-year review of the Sexual Abuse and Assault Prevention and Intervention (SAAPI) Case Management system. No changes to data collection, retention, access, or use have occurred.

ICE Enforcement and Removal Operations (ERO) Custody Management, Custody Programs (CP) Division owns the SAAPI Case Management system. SAAPI Case Management system promotes compliance with the ICE Policy No. 11062.2: Sexual Abuse and Assault Prevention and Intervention (SAAPI) (May 22, 2014), which establishes the responsibilities of ICE detention facility staff and other ICE personnel with respect to prevention, response and intervention, reporting, investigation, and tracking of incidents of sexual abuse or assault. This system facilitates oversight by the ERO CP Management Division, which has primary responsibility under this policy for incident review and reporting.

The primary function of the SAAPI Case Management system is to track the life cycle of sexual abuse and assault allegations occurring in ICE detention facilities, hold rooms, and other forms of custody. The system is used to input data about incidents and provide transparency to system users about an allegation's status. In addition, the system will allow users to follow progress about a particular incident and ensure that ICE policy requirements are being met. Lastly, the data in the system is used for collecting sexual abuse and assault allegation metrics and reporting aggregate sexual abuse and assault allegations.

Although ICE has two existing systems that may contain information about incidents of sexual abuse or assault, the SAAPI Case Management systems stores more detailed case information and performs different functions than these other systems (Joint Intake Case Management System (JICMS) and the Significant Event Notification (SEN) database). JICMS is used to track the investigation component of the allegation, which is not captured in the SAAPI Case Management system. The SEN database's primary function is to notify the appropriate ICE stakeholder of the basic information surrounding an allegation, which is contained in freeform text fields and is not standardized. The SAAPI Case Management system standardizes SEN reports by generating a report that can be copied and pasted into the SEN's freeform text field. Finally, unlike JICMS and SEN, the SAAPICM will store the results of the investigation, which are relevant to a sexual abuse or assault allegation, along with all applicable response and intervention information.

Access. The SAAPI Case Management system is built using SharePoint 2010 with strict access controls and appropriate banners to signify the presence of sensitive personally identifiable information (SPII). Access to SAAPI will be based on roles ICE personnel have in the submission and oversight process (these are defined in the Sexual Abuse and Assault Prevention and Intervention Policy). Site access will be granted to designated Prevention Sexual Assault Coordinators (PSACs) at the field office and ICE Headquarters levels. Access at ICE Headquarters is granted to the Lead PSACs from the Office of Professional Responsibility, Office of Detention Policy and Planning, and ERO Custody Programs. Data maintained on the site will be displayed in user-specific views, where the user will have access only to the case information that is most relevant to their responsibilities.

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

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): ICE ☒ Contractors working on behalf of DHS ☐ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?

The SAAPI Case Management system SharePoint site will automatically assign a unique case reference number for all sexual abuse and assault allegation cases submitted by field offices. In addition, information collected and stored includes the following:

1. Identifying information pertaining to the alleged victim and perpetrator, including full name, and as appropriate, Alien File Number, country of birth, date of birth, gender, self-identification as LGBTI, any pertinent disabilities, and primary language spoken.
2. Information determined to be relevant to the allegation, reporting timeline, and investigative findings, including description of the alleged incident, responsible investigating party (for example, DHS Office of the Inspector General, ICE Office of Professional Responsibility, ERO Administrative Inquiry Unity), sanctions or punishment enforced on the abuser (such as segregation, transfer to a different facility, or loss of privileges), incident details (location, date

[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.

[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.

and time). Witness biographical information will also be captured, including full name, and person type (e.g., ICE employee, contractor, or volunteer).	
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: Alien Number, SAAPI tracking number, and victim first and last name
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:	N/A
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	N/A
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.	
N/A	

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: Segregation Review Management System (SRMS) is another SharePoint site managed by ERO Detention Evaluation and Analysis Division. Because most sexual abuse and assault allegations will result in segregation cases separating the perpetrators and victims, SAAPI will store links to

[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.

	corresponding SRMS cases as a source of additional information. Significant Event Notification (SEN) system: sexual abuse and assault allegations on recorded in SEN and a daily list is provided to PSACs for the appropriate field office. This information is logged into the SAAPI case management system. EARM: On the rare occasion that information about the individual is missing from the SIR report, information contained in EARM will be used to complete the individual's profile in SAAPI.
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: N/A
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: Role-based training has been developed and will be deployed to both field users and ERO headquarters users. The training will emphasize the sensitive nature of the information in the database, among other matters.
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☐ No. What steps will be taken to develop and maintain the accounting: ☒ Yes. In what format is the accounting maintained: Information maintained in the system is not shared with external parties. However, when an incident is reported to local law enforcement or to a state and local services agency, it is done telephonically, and the date, time, and name of the organization or agency contacted is recorded in the system.

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:	**Nicole LaCicero**
Date submitted to Component Privacy Office:	**October 18, 2018**
Date submitted to DHS Privacy Office:	November 2, 2018

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed.

ICE Privacy recommends that the SAAPI Case Management has PIA coverage under DHS/ICE/PIA-043, SharePoint Matter Tracking Systems and under a forthcoming Appendix. ICE Privacy recommends that SAPPI has SORN coverage for information retrieved from SEN under DHS/ICE-009, External Investigations, and for information retrieved from SRMS and EARM is covered under DHS/ICE-011, Criminal Arrest Records and Immigration Enforcement Records (CARIER).

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

[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.

DHS Privacy Office Reviewer:	**Hannah Burgess**
PCTS Workflow Number:	Click here to enter text.
Date approved by DHS Privacy Office:	November 14, 2018
PTA Expiration Date	November 14, 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:	**PIA Appendix update required** If covered by existing PIA, please list: Forthcoming appendix to DHS/ICE/PIA-043 SharePoint Matter Tracking Systems
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ICE-009 External Investigations January 5, 2010 75 FR 404; DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records October 19, 2016, 81 FR 72080

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

ICE is submitting this PTA to discuss the Sexual Abuse and Assault Prevention and Intervention (SAAPI) Case Management system, which is used to track the lifecycle of sexual abuse and assault allegations occurring in ICE detention facilities, hold rooms, and other forms of custody. The system is used to input

data about incidents, track allegations/incidents, and to collect abuse and assault allegation metrics for aggregate reporting.

The DHS Privacy Office finds this is a privacy sensitive system, requiring PIA coverage as it collects PII from members of the public. Coverage will be provided under a forthcoming appendix to DHS/ICE/PIA-043 SharePoint Matter Tracking System.

SORN coverage is also required, and is provided by DHS/ICE-009 External Investigations, which covers information retrieved from the Significant Event Notification system, and by DHS/ICE-001 CARIER, which covers information retrieved from SRMS and EARM.