



Privacy Threshold Analysis

Version number: 06-2020

Page 1 of 15

PRIVACY THRESHOLD ANALYSIS (PTA)

This form will be used to determine whether a Privacy Impact Assessment (PIA), System of Records Notice (SORN), or other privacy compliance documentation is required under the E-Government Act of 2002, the Homeland Security Act of 2002, the Privacy Act of 1974, or DHS policy.

Please complete this form and send it to your Component Privacy Office. If you are unsure of your Component Privacy Office contact information, please visit <https://www.dhs.gov/privacy-office-contacts>. If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
DHS Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
(b)(6)

(b)(6)

Your Component Privacy Office will submit the PTA on behalf of your office. Upon receipt from your Component Privacy Office, the DHS Privacy Office will review this form. If a PIA, SORN, or other privacy compliance documentation is required, your Component Privacy Office, in consultation with the DHS Privacy Office, will send you a copy of the template to complete and return.

For more information about the DHS Privacy compliance process, please see <https://www.dhs.gov/compliance>. A copy of the template is available on DHS Connect at

(b)(5) or directly from the DHS Privacy Office via email: (b)(6) or phone: (b)(6)



Privacy Threshold Analysis

Version number: 06-2020

Page 2 of 15

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	Evaluate Current Threat Assessments and Threat Management – Test Efficacy		
Component or Office:	Science and Technology (S&T)	Office or Program:	MCS / PSVP
FISMA Name (if applicable):	N/A	FISMA Number (if applicable):	N/A
Type of Project or Program:	New project	Project or program status:	Development
Date first developed:	August 25, 2021	Pilot launch date:	4 months after award
Date of last PTA update	N/A	Pilot end date:	TBD
ATO Status (if applicable):¹	N/A	Expected ATO/ATP/OA date (if applicable):	N/A

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b)(6)		
Office:	Mission Capability Support	Title:	Program Manager
Phone:	(b)(6)	Email:	(b)(6)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Click here to enter text.		
Phone:	Click here to enter text.	Email:	Click here to enter text.

SPECIFIC PTA QUESTIONS

¹ The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see

(b)(5)



1. Reason for submitting the PTA: New PTA

Purpose

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) submits this new PTA to document and assess an effort from S&T's Public Safety and Violence Prevention (PSVP) program, and its contractor the National Counterterrorism, Innovation, Technology, and Education Center of Excellence, led by the University of Nebraska at Omaha (NCITE/UNO), to evaluate Current Threat Assessments and Threat Management. Findings from these evaluations will allow S&T to provide protocols for the development and utilization of new risk assessment techniques and recidivism reduction programming where current methods are found to be lacking.

Background

The science behind threat assessment and risk assessment has grown rapidly in recent years. Tools and approaches to making decisions around potential threats have evolved indicating a shifting landscape around forms and approaches to assessments. Although some support tools exist, the overall validity of threat assessment tools and models is tentative as it is unclear whether potential threats would fail to be identified using current threat models in existence.

S&T works closely with other DHS Components, such as the United States Secret Service (USSS) and as per priority action 3.3.6 of the DHS Strategic Framework for CTTV (October 2020), S&T is lead for expanding efforts to evaluate prevention programs. Considering the above observations of the threat assessment literature, models, and approaches, we seek to accomplish the below goals in this activity's evaluation:

1. Conduct an outcome evaluation and testing on the general quality and role of threat assessments and threat management programs to determine whether or not these efforts were successful in achieving its intended objectives
2. Conduct an impact evaluation to measure intended and unintended changes that can be attributed to the implementation and outcomes of various threat assessments and models.

The goal of this evaluation is to advance science forward, as efforts mature from previous work. To do so, we will focus on potential capability gaps that may be ameliorated by considering unique and alternative perspectives.

Evaluation of Threat Assessments and Threat Management

DHS S&T has contracted this activity to NCITE/UNO, who will conduct an outcome and impact evaluation of current threat assessment tools and threat management techniques in order to validate whether or not these efforts were successful in diversion and recidivism. Findings from these outcome and impact evaluations will allow S&T to provide protocols for the development and utilization of new risk assessment techniques and recidivism reduction programming where current methods are found to be lacking.

S&T will work with NCITE/UNO to design and develop assessment approaches, protocols and measurement tools that will be used to determine unique demands and needs of the security community.



Findings from these evaluations aim to provide scientific evidence to inform research, design, and assistance to federal (specifically USSS), state, local law enforcement, as well as 5RD partners, CP3, and DHS Policy.

Data Sources and Methods

S&T will use a multidisciplinary approach where applied tools and techniques in evaluation research are utilized. NCITE/UNO researchers will:

- Review threat assessment literature
- Provide and leverage insight from allies in the United Kingdom (UK) from previous evaluation work conducted by NCITE/UNO
- Gain a better understanding of contrasting approaches between foreign allies (UK) and domestic security agencies such as those taken by USSS.
- Gather insights from lesson learned from local and state LE personnel.
- Review threat assessments on insider threats
- Examine current threat assessment approaches for potential gaps dealing with novel threats.

The research team will employ a range of methods in searching for and synthesizing the evidence around threat assessment and threat models. The focus shall be on principles of information science and coding strategies used in systematic searches. Once the literature, which will consist of academic studies and publications, grey literature, etc., has been sourced, NCITE/UNO researchers and S&T will determine a synthesis (meta-analysis, qualitative, etc.) strategy.

The research team will facilitate a kick-off meeting at the beginning of the activity to produce an agreed approach to determine the methodology(s) to be used for the review. A protocol will be produced prior to completion of the review to provide a brief background to the subject, indicate that DHS is sponsoring the research, and to show the research's value for policy and practice. This will inform discussions with practitioners to ensure that the review meets its intended objectives.

Through case analysis, survey-embedded experiments², and interviews (both virtual and in person), the research team will identify commonly used tools, reactions and attitudes towards those tools, and how the tools themselves are used and applied. Sample questions will request information on participant's current threat assessment process, and how they cooperate with other agencies.

All potential research subjects must be 19 years of age or older and utilize threat assessment tools as part of their job responsibilities. This may include members of the Secret Service, other United States government personnel, and threat assessment personnel at the local and federal level. They will be assigned an anonymous identifier to protect identifiable and private information.

The project will involve engagement with individuals involved in threat assessment at the federal, state and local level. NCITE will collect and use the following information from these individuals:

- Names,
- Email address, and

² This refers to an experiment conducted within a survey in which the researcher will randomly assign participants at least two experimental conditions. By treating each condition differently due to the random assignment, researchers can assume the only difference between conditions is the difference in reactions/attitudes.



- Telephone numbers

NCITE will collect and use this information for the sole purpose of facilitating participation in the evaluation effort. NCITE will not share any of this information with S&T.

After an initial design and development phase collecting process information, the research team will determine if more detailed data describing outcomes can be collected. The research team will develop IRB amendments and modifications to all privacy documentation if the research team determines additional data collection is possible.

The case analyses, surveys analysis, structured interviews, and document reviews will allow for a comprehensive literature review and summary on current approaches for assessments. The summary report will integrate findings from interviews with IRB, Privacy and CAPO approvals taking place prior to data collection beginning.

Researchers will work in collaboration with S&T to:

1. Design, develop, and facilitate interviews, case analysis, and structured surveys to identify commonly used tools, reactions, and attitudes towards those tools, and how they are used and applied. The specific interview questions are:
 - a. What is your background as a practitioner?
 - b. What is your previous threat assessment experience?
 - c. Given your expertise in threat assessment, what are your suggestions for the improvement of current tools and approaches?
 - d. What are you current preferred threat assessment tools or general approaches?
 - e. What is your perception around the utility of tools in supporting threat assessment?
2. Set priorities and expectations with S&T and participating stakeholders (such as USSS).
3. Develop protocols, instruments, and data transfer/use agreements (such as anonymized survey/interview data) with participating stakeholders.
4. Develop protocols to guide structured interviews with participating stakeholders.

Data Management

All researchers involved in the proposed study will monitor and supervise the safety of any data collected, although ultimate responsibility will fall to the Principal Investigation (PI) at UNO/NCITE. The PI and other researchers involved will clearly define and commit to data quality and safety protocols per the UNO Institutional Review Board (IRB) and project plan.

The research data and all files and documentation, such as descriptions of the study design, data collection forms, IRB documentation, CABLab data, etc. will be saved on NCITE servers at the UNO site. Access to this data will only be granted to members of the research team through locked doors with key card entry and will be destroyed at the conclusion of the activity.

Reports

Upon completion of the effort, DHS S&T shall receive a final report, detailing the findings of the evaluation of the threat and risk assessments which will be provided directly to participating stakeholders from the study. Due to the nature and any national/state security concerns, recommendations will not be made publicly available. These reports will not contain any PII, and information will only be reported in aggregate form to protect individual privacy.



Privacy Threshold Analysis

Version number: 06-2020

Page 6 of 15

2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? <i>Please check all that apply.</i>	☐ This project does not collect, collect, maintain, use, or disseminate any personally identifiable information³ ☒ Members of the public ☒ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons State and local threat assessment personnel who volunteer to participate in this research. No attempt is made to ascertain the citizenship status of these individuals. ☒ DHS Employees/Contractors (list Components): USSS, others TBD ☒ Other federal employees or contractors (list agencies): TBD
2(a) Is information meant to be collected from or about sensitive/protected populations?	☒ No ☐ 8 USC § 1367 protected individuals (e.g., T, U, VAWA)⁴ ☐ Refugees/Asylees ☐ Other. Please list: <i>Click here to enter text.</i>

3. What specific information about individuals is collected, maintained, used, or disseminated?
The project will involve engagement with individuals via meetings (or online equivalents, due to COVID19) involved in threat assessment at the federal (as part of their work duties), state and local level. NCITE will collect and use the following information from these individuals:

³ 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 This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, *available at*

(b)(5)



Privacy Threshold Analysis

Version number: 06-2020

Page 7 of 15

- Names,
- Email address, and
- Telephone numbers

NCITE will collect and use this information for the sole purpose of facilitating participation in the evaluation effort.

IRB and privacy documents will be amended and modified if researchers determine additional PII-related data is necessary.

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?⁵ If applicable, check all that apply.

- ☐ Social Security number
- ☐ Alien Number (A-Number)
- ☐ Tax Identification Number
- ☐ Visa Number
- ☐ Passport Number
- ☐ Bank Account, Credit Card, or other financial account number
- ☐ Driver's License/State ID Number

- ☐ Social Media Handle/ID
- ☐ Driver's License/State ID Number
- ☐ Biometric identifiers (e.g., *FIN, EID*)
- ☐ Biometrics.⁶ Please list modalities (e.g., *fingerprints, DNA, iris scans*): Click here to enter text.
- ☐ Other. Please list: Click here to enter text.

3(b) Please provide the specific legal basis for the collection of SSN:

N/A

3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.

N/A

3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,⁷ which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as

⁵ Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, available at (b)(5)

⁶ If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.

⁷ See (b)(5)



Privacy Threshold Analysis

Version number: 06-2020

Page 8 of 15

<i>masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.</i>
N/A

4. How does the Project, Program, or System retrieve information?	☒ By a unique identifier.⁸ Please list all unique identifiers used: NCITE may retrieve information about participants such as name, phone number, or email address for the purpose of facilitating participation in the study. ☒ By a non-unique identifier or other means. Please describe: NCITE will develop unique identifiers for the practitioners participating in the surveys and interviews. A crosswalk between the unique identifier and the volunteer's information will be maintained separately. This will be maintained only for the duration of the project in case the NCITE has to reference it later in the project
---	---

5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)? If no schedule has been approved, please provide proposed schedule or plans to determine it. <i>Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.⁹</i>	UNO will adhere to the record retention policies of the IRB of Record. As stated above, any PII UNO collects or uses as part of this effort will be destroyed after 7 years.
5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)?	Manual Audit. PI is responsible for data management and will monitor compliance.

⁸ Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which 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.

⁹ See (b)(5)



Privacy Threshold Analysis

Version number: 06-2020

Page 9 of 15

6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?¹⁰	☒ No. ☐ Yes. If yes, please list:
7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?	☒ No. ☐ Yes. If yes, please list: <i>Click here to enter text.</i>
8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? If applicable, please provide agreement as an attachment.	N/A Please describe applicable information sharing governance in place: <i>Click here to enter text.</i>
9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?	☒ No. What steps will be taken to develop and maintain the accounting: NCITE will not make any disclosures of an individual's PII outside of the NCITE project team. As a result, there are no disclosures to be tracked. ☐ Yes. In what format is the accounting maintained: <i>Click here to enter text.</i>
10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☐ Social Media ☐ Advanced analytics ¹¹ ☐ Live PII data for testing ☒ No
11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic	☒ No.

¹⁰ 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 IACS.

¹¹ The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.



Privacy Threshold Analysis

Version number: 06-2020

Page 10 of 15

database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)? ¹² This does not include subject-based searches.	☐ Yes. If yes, please elaborate: <i>Click here to enter text.</i>
11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	☒ No. ☐ Yes. If yes, please elaborate:
12. Does the planned effort include any interaction or intervention with human subjects ¹³ via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for <u>research purposes</u>	☐ No. ☒ Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for <u>independent</u> review and approval of this effort. ¹⁴
13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, <u>in addition</u> to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: NCITE will include security and privacy certificates that complies with the requirements of the Privacy Act.
14. Is there a FIPS 199 determination? ¹⁵	☒ No.

¹² Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a Government agency or program; or

(ii) the security of a Government computer system.

¹³ Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

¹⁴ For more information about CAPO and their points of contact, please see: (b)(5)

(b)(5) or (b)(5) For more information about the protection of human

subjects, please see DHS Directive 026-04: (b)(5)

(b)(5)

¹⁵ 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.



Privacy Threshold Analysis
Version number: 06-2020
Page 11 of 15

	☐ 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:	John Lambert, Senior Privacy Specialist Sean J. Vanek, Contract Support Privacy Analyst
Date submitted to Component Privacy Office:	Click here to enter a date.
Concurrence from other Component Reviewers involved (if applicable):	N/A
Date submitted to DHS Privacy Office:	November 15, 2021
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.</i>	
The S&T Privacy Office submits this new PTA to document and assess an effort from S&T's Public Safety and Violence Prevention (PSVP) program, and its contractor the National Counterterrorism, Innovation, Technology, and Education Center of Excellence, led by the University of Nebraska at Omaha (NCITE/UNO), to evaluate Current Threat Assessments and Threat Management. Findings from these evaluations will allow S&T to provide protocols for the development and utilization of new risk assessment techniques and recidivism reduction programming where current methods are found to be lacking. DHS S&T has contracted this activity to NCITE/UNO, who will conduct an outcome and impact evaluation of current threat assessment tools and threat management techniques in order to validate whether or not these efforts were successful in diversion and recidivism. Findings from these outcome and impact evaluations will allow S&T to provide protocols for the development and utilization of new risk assessment techniques and recidivism reduction programming where current methods are found to be lacking. The research team will employ a range of methods in searching for and synthesizing the evidence around threat assessment and threat models. The focus shall be on principles of information science and coding strategies used in systematic searches. Once the literature, which will consist of academic studies and publications, grey literature, etc., has been sourced, NCITE/UNO researchers and S&T will determine a synthesis (meta-analysis, qualitative, etc.) strategy. Through case analysis, survey-embedded experiments, and interviews (both virtual and in person), the research team will identify commonly used tools, reactions and attitudes towards those tools, and how the tools themselves are used and applied. Sample questions will request information on participant's current threat assessment process, and how they cooperate with other agencies. All potential research subjects must be 19 years of age or older and utilize threat assessment tools as part of their job responsibilities. This may include members of the Secret Service, other United States government personnel, and threat assessment personnel at the local and federal level. They will be assigned an anonymous identifier to protect identifiable and private information.	



Privacy Threshold Analysis

Version number: 06-2020

Page 13 of 15

The project will involve engagement with individuals involved in threat assessment at the federal, state and local level. NCITE will collect and use the following information from these individuals:

- Names,
- Email address, and
- Telephone numbers

NCITE will collect and use this information for the sole purpose of facilitating participation in the evaluation effort. NCITE will not share any of this information with S&T.

The S&T Privacy Office recommends that this effort is privacy sensitive and that the following privacy compliance documentation provides sufficient coverage:

PIA:

DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups, which covers how NCITE will collect information that to facilitate interviews.

SORN:

DHS/ALL-002 Department of Homeland Security Mailing and Other Lists, which covers the business contact information NCITE may retrieve for the purposes of facilitating interview activities.



Privacy Threshold Analysis

Version number: 06-2020

Page 14 of 15

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Kattina Do
DHS Privacy Office Approver (if applicable):	Riley Dean
Workflow Number:	0022017
Date approved by DHS Privacy Office:	February 25, 2022
PTA Expiration Date	February 25, 2025

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	New Project If “other” is selected, please describe: Click here to enter text.
Determination:	☒ Project, Program, System in compliance with full coverage ☐ Project, Program, System in compliance with interim coverage ☐ Project, Program, System in compliance until changes implemented ☐ Project, Program, System not in compliance
PIA:	System covered by existing PIA DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups
SORN:	System covered by existing SORN DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.</i>	
S&T is submitting this PTA to discuss the Evaluate Current Threat Assessments and Threat Management – Test Efficacy. This PTA is to document and assess an effort from S&T’s Public Safety and Violence Prevention (PSVP) program, and its contractor the National Counterterrorism, Innovation, Technology, and Education Center of Excellence, led by the University of Nebraska at Omaha (NCITE/UNO), to evaluate Current Threat Assessments and Threat Management. Findings from these evaluations will allow S&T to provide protocols for the development and utilization of new risk assessment techniques and recidivism reduction programming where current methods are found to be lacking. The science behind threat assessment and risk assessment has grown rapidly in recent years. Tools and approaches to making decisions around potential threats have evolved indicating a shifting landscape around forms and approaches to assessments. Although some support tools exist, the overall validity of	



Privacy Threshold Analysis

Version number: 06-2020

Page 15 of 15

threat assessment tools and models is tentative as it is unclear whether potential threats would fail to be identified using current threat models in existence.

S&T works closely with other DHS Components, such as the United States Secret Service (USSS) and as per priority action 3.3.6 of the DHS Strategic Framework for CTTV (October 2020), S&T is lead for expanding efforts to evaluate prevention programs. Considering the above observations of the threat assessment literature, models, and approaches, we seek to accomplish the below goals in this activity's evaluation: conduct an outcome evaluation and testing on the general quality and role of threat assessments and threat management programs to determine whether or not these efforts were successful in achieving its intended objectives, and conduct an impact evaluation to measure intended and unintended changes that can be attributed to the implementation and outcomes of various threat assessments and models. The goal of this evaluation is to advance science forward, as efforts mature from previous work. To do so, we will focus on potential capability gaps that may be ameliorated by considering unique and alternative perspectives.

The project will involve engagement with individuals via meetings (or online equivalents, due to COVID19) involved in threat assessment at the federal (as part of their work duties), state and local level. NCITE will collect and use the following information from these individuals: names, email address, and telephone numbers. NCITE will collect and use this information for the sole purpose of facilitating participation in the evaluation effort. IRB and privacy documents will be amended and modified if researchers determine additional PII-related data is necessary.

The DHS Privacy Office (PRIV) agrees that this new project is privacy-sensitive, requiring PIA and SORN coverage because PII is collected from members of the public, DHS personnel, and other federal employees.

PRIV agrees with S&T Privacy that PIA coverage is provided by DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups provides transparency into the privacy risks associated with DHS's collection, maintenance, and use of PII in order to facilitate correspondence via a survey.

SORN coverage is required because information is retrieved by personal identifier. PRIV agrees with S&T Privacy that SORN coverage is provided by DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, which covers the lists used to facilitate mailings to multiple addressees and other activities in furtherance of DHS duties.

Any updates to the project will require an update to this PTA.