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:	**National Emergency Communications Plan (NECP)**		
Component:	**National Protection and Programs Directorate (NPPD)**	**Office or Program:**	**Cyber Security & Communications (CS&C) Office of Emergency Communications (OEC)**
Xacta FISMA Name (if applicable):	**National Emergency Communications Plan (NECP)**	**Xacta FISMA Number (if applicable):**	TBD
Type of Project or Program:	**IT System**	**Project or program status:**	**Development**
Date first developed:	Click here to enter a date.	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable)	**In progress**	**ATO expiration date (if applicable):**	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	**Kendall Carpenter**		
Office:	**CS&C, OEC, Technical Assistance Branch**	**Title:**	**Telecommunications Specialist**
Phone:	**(202) 744-1580**	**Email:**	**Kendall.carpenter@dhs.gov**

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	**Larry L. Willis**		
Phone:	**(202) 557-5934**	**Email:**	**Larry.L.Willis@HQ.DHS.GOV**

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Choose an item.

The National Protection and Programs Directorate (NPPD), Office of Cyber Security & Communications (CS&C), Office of Emergency Communications (OEC) is conducting this PTA to discuss the privacy compliance and Paperwork Reduction Act (PRA) requirements for OEC services supporting the implementation activities of the National Emergency Communications Plan (NECP). This PTA will introduce the Communication Assets Survey and Mapping (CASM) tool, and update and replace previously adjudicated PTAs for the following activities, to roll them up under the larger NECP. These are:

- NECP Statewide Communications Interoperability Plan (SCIP) (August 26, 2013);
- Communications Unit Leader (COML) (November 24, 2010),
- OEC Technical Assistance Request and Evaluation (TARE) (October 20, 2013)

The OEC, was formed under Title XVIII of the Homeland Security Act of 2002, 6 U.S.C. § 101 et seq., as amended, and pursuant to the goals and initiatives outlined in the NECP.
OEC is required to develop and maintain the NECP, which includes identification of goals, milestones, timeframes, and appropriate measures to achieve interoperable communications capabilities among inter and intrastate emergency responders.

The vision of the NECP is to ensure emergency response personnel at all levels of government, and across disciplines, can communicate as needed, on demand, and as authorized. To achieve this vision, the NECP identifies the capabilities and initiatives needed for communications operability, interoperability, and continuity of communications for emergency responders nationwide.
OEC has a statutory requirement to implement the NECP and provide technical assistance and emergency communications-related services at no charge to state, federal, regional, local, and tribal government officials.

The NECP service areas identified by statutory requirements for this PTA are:

Statewide Communications Interoperability Plan (SCIP)

The NECP recommends that all 56 States/territories develop and maintain a SCIP. OEC's Technical Assistance (TA) Branch provides TA services and Statewide Planning for all 56 State/Territories supporting the implementation of the NECP and their respective SCIPs.

In 2010, the Statewide Communication Interoperability Plan (SCIP) Implementation Report was cleared in accordance with the Paperwork Reduction Act of 1995. The SCIP Template and SCIP Snapshot will replace the previous SCIP Template and SCIP Annual Progress Report. These updated documents (SCIP Template and SCIP Snapshot) streamline the information collected by OEC to track the progress states are making in implementing milestones and demonstrating goals of the NECP. There is no change to the information being collected; there is no PII collected/stored for NECP SCIP. The only proposed change to the collection is that an online option is being added which will allow States the option of submitting both documents via email at *oec@hq.dhs.gov* or through an online tool (eSCIP - under development).

The SCIP Template and SCIP Snapshot will assist states in their strategic planning for interoperable and emergency communications while demonstrating each state's achievements and challenges in accomplishing optimal interoperability for emergency responders. In addition, certain government grants may require states to update their SCIP Templates and SCIP Snapshot Reports to include broadband efforts in order to receive funding for interoperable and emergency communications.

Statewide Interoperability Coordinators (SWICs) will be responsible for the development and incorporation of input from their respective stakeholders and governance bodies into their SCIP Template and SCIP Snapshot. SWICs will complete and submit the reports directly to OEC through unclassified electronic submission. SWIC POC information will be managed at the state/local level; PII will NOT be collected, maintained, or managed at the DHS/NPPD/CS&C/OEC level.

Technical Assistance Request and Evaluation (TARE)

OEC formed under Title XVIII of the Homeland Security Act of 2002, 6 U.S.C.574 *et seq.*, as amended, is authorized to provide technical assistance at no charge to State, regional, local, and tribal government officials. OEC will use the Technical Assistance Requests to identify the number and type of technical assistance requests from each State and territory. OEC will use the Technical Assistance Evaluation to support quality improvement of its technical assistance services. Updated forms are pending through the Paperwork Reduction Act (PRA) Process.

Fillable electronic copies of the TA forms will be available on line at: www.publicsafetytools.info [1]and only authorized SWICs or their representative, recognized by OEC can complete and submit the form on-line. The information collected for TARE remains the same as previously identified; the following information about individuals is collected: name, title, agency, fax number, and email address. Upon completion, the form is sent electronically to a DHS at: TARequest@hq.dhs.gov. TA forms are saved to a DHS OEC NECP access controlled SharePoint site.

Communications Assets and Survey Mapping (CASM) Tool

Per the NECP requirements, OEC provides the CASM tool, accessible by SWICs, via www.publicsafetytools.info. NECP Initiative 1.3 “makes available an effective communications asset management tool containing security and privacy controls to allow for nationwide intergovernmental use.” CASM supports tactical planning among Federal, State, local and tribal governments at the regional interstate level. Access to State/territory CASM accounts are controlled by the respective SWIC for their State/territory and all new user requests are sent via email from the requester directly to the SWIC. DHS has only administrative access to information

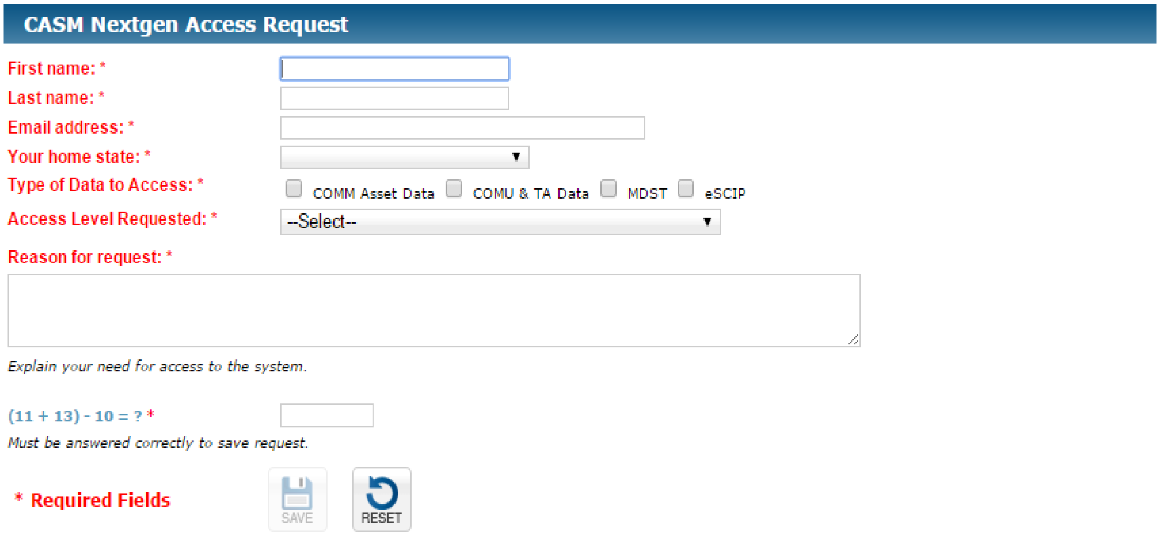
[1] OEC is working with CS&C Information Assurance (IA) for the publicsafetytools.info web site to move it into a FEDRAMP/DHS (4300a) compliant posture.

provided by the SWICs for the respective State/territory. Under DHS oversight, SPAWAR maintains control/security of the system containing CASM information.

CASM Access

In order to receive an account to receive access to CASM and provide input other SWICs within their state/territory, SWICs must request access via the CASM Nextgen Access Request form (shown below). Information is collected and maintained through an Inter-Agency Agreement (IAA) between DHS and the Department of Defense (DoD), Space and Naval Warfare Systems Command (SPAWAR) San Diego[2].

The table below shows the current CASM access request. Users will select their type of access: Communication Assets (COMM Asset) Data, COMU & TA Data, (National Public Safety Broadband Network's) Mobile Data Survey Tool (MDST), and eSCIP. This form will be updated with a Privacy Act Statement and be processed through the PRA process.



CASM Nextgen Access Request

First name: *

Last name: *

Email address: *

Your home state: *

Type of Data to Access: * □ COMM Asset Data □ COMU & TA Data □ MDST □ eSCIP

Access Level Requested: * --Select--

Reason for request: *

Explain your need for access to the system.

(11 + 13) - 10 = ? *

Must be answered correctly to save request.

* Required Fields

Communications Unit (COMU) Training

OEC in accordance with the NECP fosters the development of interoperable emergency communications capabilities for State, regional, local, and tribal governments and addresses these responsibilities, in part, by offering All Hazards Communications Unit training courses for state, regional, and local emergency response stakeholders. Participation in these courses requires

[2] OEC is working with CS&C IA to ensure data managed by DoD/SPAWAR moves into a FEDRAMP/DHS (4300a) to maintain FISMA security and privacy compliance posture.

satisfaction of several prerequisites that the States/territories verify for their nominated students. COMU students provide contact information[3] (Name, business affiliation (i.e. State, Agency, and Discipline), Mailing Address, email & Phone Number) to the SWIC that is then entered into CASM.

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[4] (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[5] ☒ 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?

[3] Contact information provided is only used to document attendance and provide a certificate of completion. OEC NECP does not retrieve COMU student information by personal identifier. Student information can only be retrieved by state, course title, and date.

[4] 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.

[5] 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.

Please provide a specific description of information that is collected, generated, or retained (such as names, addresses, emails, etc.) for each category of individuals.

NECP collects contact information only (Name, business affiliation (i.e. State, Agency, and Discipline), Mailing Address, email & Phone Number).

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: Information can be retrieved by user contact information (name, title, agency, fax number, and/or email address)
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.
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[6] 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	☒ No.

[6] 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.

other DHS programs or systems[7]?	□ 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:
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: Access to and updates for State/territory CASM accounts are controlled by the respective SWIC for their State/territory and all new/updated user requests are sent via email from the requester directly to the SWIC. DHS has only administrative access to information provided by the SWICs for the respective State/territory. □ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[8]	□ Unknown. □ No. ☒ Yes. Please indicate the determinations for each

[7] 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.

[8] 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.

	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:	**Cindy Falkenstein**
Date submitted to Component Privacy Office:	**April 2, 2015**
Date submitted to DHS Privacy Office:	April 2, 2015
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
NPPD is conducting this PTA to update and replace the activities of the: NECP SCIP PTA, adjudicated August 26, 2013; the COML PTA, adjudicated November 24, 2010, and the OEC TARE PTA, adjudicated October 20, 2013, and to introduce the CASM tool. Because the activities described herein includes the collection of contact information of emergency response personnel at all levels of government, and across disciplines, NPPD Office of Privacy recommends that the activities as described shall be considered privacy sensitive and that a new PIA is not required and can be covered by the existing DHS-Wide General Contacts List PIA and DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System (SORN), and DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792 This is a FISMA/Xacta system and this PTA will need to be uploaded into Xacta once adjudicated.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Emily Andrew, NPPD Senior Privacy Officer

PCTS Workflow Number:	**1077272**
Date approved by DHS Privacy Office:	April 2, 2015
PTA Expiration Date	April 2, 2018

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-Wide General Contacts List PIA
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System (SORN), and DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792

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

NPPD is conducting this PTA to update and replace the activities of the: NECP SCIP PTA, adjudicated August 26, 2013; the COML PTA, adjudicated November 24, 2010, and the OEC TARE PTA, adjudicated October 20, 2013, and to introduce the CASM tool.

NPPD Office of Privacy recommends that the activities as described shall be considered privacy sensitive and that a new PIA is not required and can be covered by the existing DHS-Wide General Contacts List

PIA and DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System (SORN), and DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792.
PA Statements provided for PS Form 9042, PS Form 9043 and the CASM tool (PS Form TBD) have been reviewed and approved. NPPD Privacy should ensure that these PA Statements are implemented as appropriate.

NPPD Privacy should also work with CS&C through the PRA process.

The following PTAs will be retired and documented in the DHS Privacy Office compliance inventory:
NECP SCIP PTA, adjudicated August 26, 2013;
COML PTA, adjudicated November 24, 2010: and
OEC TARE PTA, adjudicated October 20, 2013.