



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:

Rebecca J. Richards
Senior Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@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@dhs.gov, phone: 703-235-0780.



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)
TAFISMA Name:	N/A	TAFISMA Number:	N/A
Type of Project or Program:	Notice of Proposed Rulemaking/Final Rule	Project or program status:	Update

PROJECT OR PROGRAM MANAGER

Name:	Serena Maxey		
Office:	CS&C, OEC, Partnerships Branch, Statewide Planning	Title:	Program Specialist
Phone:	(703) 235-2822	Email:	serena.maxey@hq.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	N/A: the OEC does not own systems; an ISSO is not required		
Phone:	Click here to enter text.	Email:	Click here to enter text.

ROUTING INFORMATION

Date submitted to Component Privacy Office:	August 23, 2013
Date submitted to DHS Privacy Office:	Click here to enter a date.
Date approved by DHS Privacy Office:	Click here to enter a date.



SPECIFIC PTA QUESTIONS

1. Please describe the purpose of the project or program:

Please provide a general description of the project and its purpose in a way a non-technical person could understand.

The National Protections and Programs Directorate (NPPD), Office of Cyber Communications (CS&C), Office of Emergency Communications (OEC) is updating this PTA to satisfy the three-year privacy compliance review and to satisfy the program's PRA requirements.

OEC is required to develop and maintain the National Emergency Communications Plan (NECP), which includes identification of goals, timeframes, and appropriate measures to achieve interoperable communications capabilities. The NECP Performance Report is designed to meet the statutory requirements, to ensure 75 percent of non-Urban Areas Security Initiative (UASI) jurisdictions are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies. As part of the OEC's Partnerships Branch, Statewide Planning, the Statewide Communication Interoperability Plan (SCIP) Template and Annual Progress Report are designed to meet and support these statutory requirements.

In 2010, the SCIP Implementation Report was cleared in accordance with the Paperwork Reduction Act of 1995 and will expire in September of 2013. The SCIP Template and Annual Progress Report will replace the previous SCIP Template and SCIP Implementation Report. These updated documents (SCIP Template and Annual Progress Report Template) streamline the information collected by OEC to track the progress States are making in implementing milestones and demonstrating goals of the NECP. The process for completing the SCIP Template and Annual Progress Report will not change.

The SCIP Template and Annual Progress Report 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 Annual Progress 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 Annual Progress Report. 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.

2. Project or Program status

Choose an item.

Date first developed:	September 1, 2007	Pilot launch date:	Click here to enter a date.
Date last updated:	November 24, 2010	Pilot end date:	Click here to enter a date.

3. From whom does the Project or

DHS Employees



Privacy Threshold Analysis

Version date: July 7, 2012

Page 4 of 7

<p>Program collect, maintain, use or disseminate information? <i>Please check all that apply.</i></p>	<p><input type="checkbox"/> Contractors working on behalf of DHS</p> <p><input type="checkbox"/> Members of the public</p> <p><input checked="" type="checkbox"/> This program does not collect any personally identifiable information¹</p>
<p>4. What specific information about individuals could be collected, generated or retained? <i>Please provide a specific description of information that might be collected, generated or retained such as names, addresses, emails, etc.</i></p>	
<p>N/A</p>	
<p>Does the Project or Program use Social Security Numbers (SSNs)?</p>	<p>No</p>
<p>If yes, please provide the legal authority for the collection of SSNs:</p>	<p>Click here to enter text.</p>
<p>If yes, please describe the uses of the SSNs within the Project or Program:</p>	<p>Click here to enter text.</p>
<p>5. Does this system employ any of the following technologies: <i>If project or program utilizes any of these technologies, please contact Component Privacy Officer for specialized PTA.</i></p>	<p><input type="checkbox"/> Closed Circuit Television (CCTV)</p> <p><input type="checkbox"/> Sharepoint-as-a-Service</p> <p><input type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Mobile Application (or GPS)</p> <p><input type="checkbox"/> Web portal²</p> <p><input checked="" type="checkbox"/> None of the above</p>
<p>If this project is a technology/system, does it relate solely to infrastructure? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i></p>	<p><input checked="" type="checkbox"/> No. Please continue to next question.</p> <p><input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.</p>
<p>If header or payload data³ is stored in the communication traffic log, please detail the data elements stored.</p>	

¹ 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.

² Informational and collaboration-based portals in operation at DHS and its components which collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are “members” of the portal or who seek to gain access to the portal “potential members.”



Click here to enter text.	
6. Does this project or program connect, receive, or share PII with any other DHS programs or systems⁴?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: Click here to enter text.
7. Does this project or program connect, receive, or share PII with any external (non-DHS) partners or systems?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: Click here to enter text.
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. Click here to enter text.

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 TAFISMA.



PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Emily Andrew
Date submitted to DHS Privacy Office:	August 26, 2013
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
This PTA is being conducted to satisfy the three-year privacy compliance review and the program's Paperwork Reduction Act requirements. The program does not collect or share PII; the NPPD Office of Privacy recommends designating this as <u>NOT a Privacy Sensitive System.</u>	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Liz Lyons
Date approved by DHS Privacy Office:	September 3, 2013
PCTS Workflow Number:	992653

DESIGNATION

Privacy Sensitive System:	No If "no" PTA adjudication is complete.
Category of System:	Choose an item. If "other" is selected, please describe: Click here to enter text.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input type="checkbox"/> Privacy Impact Assessment (PIA) required. <input type="checkbox"/> System of Records Notice (SORN) required.
PIA:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.
DHS Privacy Office Comments:	



**Homeland
Security**

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: July 7, 2012
Page 7 of 7

Please describe rationale for privacy compliance determination above.

Click here to enter text.