



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:	Citizens Corps (CCORPS)		
Component:	Federal Emergency Management Agency (FEMA)	Office or Program:	National Preparedness
Xacta FISMA Name (if applicable):	Citizens Corps (CCORPS)	Xacta FISMA Number (if applicable):	FEM-06753-MAJ-06753
Type of Project or Program:	Program	Project or program status:	Operational
Date first developed:	N/A	Pilot launch date:	N/A
Date of last PTA update	June 28, 2013	Pilot end date:	N/A
ATO Status (if applicable)	Complete	ATO expiration date (if applicable):	September 23, 2015

PROJECT OR PROGRAM MANAGER

Name:	Samuel Hultzman		
Office:	Protection and National Preparedness	Title:	IT Program Manager
Phone:	202-786-9866	Email:	samuel.hultzman@fema.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	John Shore		
Phone:	202-786-9638	Email:	john.shore@associates.fema.dhs.gov



SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

The Federal Emergency Management Agency (FEMA), Office of Protection and National Preparedness (PNP), Individual and Community Preparedness Division (ICPD) administer the Citizen Corps Program, which also includes the Citizen Corps web-based application, and the Citizen Corps Database. Citizen Corps' mission is to strengthen the collaboration between government and community leaders from all sectors to encourage citizens' preparedness through education, training, and volunteer service to make communities safer, stronger, and better prepared to respond to all hazards and all threats. Through Citizen Corps, communities can establish and register Citizen Corps Councils (Councils) and Community Emergency Response Team (CERT) programs. The Citizen Corps system collects personally identifiable information (PII) associated with points of contacts (POC) designated by Councils, CERTs, and other Citizen Corps partners.

This PTA is being updated because the previous adjudication of 'New PIA Required' is no longer accurate. The Citizen Corp PIA was signed June 28, 2013.

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 portal¹ (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 information²
- Members of the public
- DHS employees/contractors (list components):
FEMA.
- Contractors working on behalf of DHS

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.



	<input checked="" type="checkbox"/> Employees of other federal agencies
--	---

4. What specific information about individuals is collected, generated, or retained?	
Names, Mailing Addresses, Email Addresses, and Telephone Numbers	
4(a) Does the project, program, or system retrieve information by personal identifier?	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> 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? <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<input checked="" type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data³ is stored in the communication traffic log, please detail the data elements stored.	
N/A	

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.



<p>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems⁴?</p>	<p><input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: N/A</p>
<p>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</p>	<p><input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: N/A</p>
<p>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</p>	<p>Choose an item. Please describe applicable information sharing governance in place: N/A</p>
<p>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?</p>	<p><input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list:</p>
<p>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?</p>	<p><input type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: <input checked="" type="checkbox"/> Yes. In what format is the accounting maintained: The FEMA Disclosure Officer who maintains the accounting of what records are disclosed and to whom.</p>

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.



9. Is there a FIPS 199 determination?⁴	<input type="checkbox"/> Unknown. <input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following: Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Integrity: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined Availability: <input checked="" type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined
--	--

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Lane Raffray
Date submitted to Component Privacy Office:	March 30, 2015
Date submitted to DHS Privacy Office:	March 30, 2015
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
PIA: DHS/FEMA/PIA-029 - Citizen Corps Program	
SORN: DHS/FEMA-006 - Citizen Corps Program July 22, 2013 78 FR 43890	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Eric M. Leckey
PCTS Workflow Number:	1076311
Date approved by DHS Privacy Office:	March 31, 2015
PTA Expiration Date	March 31, 2018

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.



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:	<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 checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. <input type="checkbox"/> 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/FEMA/PIA-029 - Citizen Corps Program
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/FEMA-006 - Citizen Corps Program July 22, 2013 78 FR 43890
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
The PTA was updated because the previous PTA, adjudicated 12/18/2012, noted that a “New PIA was required.” The Citizen Corp PIA was signed June 28, 2013. This PTA was updated to reflect that privacy compliance coverage. No changes were made to the Citizen Corps SORN, DHS/FEMA-006 - Citizen Corps Program (July 22, 2013, 78 FR 43890). No further action is required at this time.	