



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:	FEMA Preparedness Grants: Port Security Grant Program (PSGP)		
Component:	Federal Emergency Management Agency (FEMA)	Office or Program:	Grant Programs Directorate (GPD) Port Security Grant Program
TAFISMA Name:		TAFISMA Number:	
Type of Project or Program:	Form or other Information Collection	Project or program status:	Operational

PROJECT OR PROGRAM MANAGER

Name:	Jeffrey Hall		
Office:	FEMA GPD	Title:	Program Analyst
Phone:	202-230-8452	Email:	Jeffrey.hall1@dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

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

ROUTING INFORMATION

Date submitted to Component Privacy Office:	May 14, 2013
Date submitted to DHS Privacy Office:	May 14, 2013
Date approved by DHS Privacy Office:	August 26, 2013



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 FEMA Grant Programs Directorate (GPD) manages the Port Security Grant Program (PSGP). The PSGP is a DHS grant program that focuses on infrastructure protection activities. The PSGP is one tool in the comprehensive set of measures authorized by Congress and implemented by the Administration to strengthen the Nation’s critical infrastructure against risks associated with potential terrorist attacks. The vast bulk of U.S. critical infrastructure is owned and/or operated by State, local and private sector partners. PSGP funds support increased port-wide risk management; enhanced domain awareness; training and exercises; and further capabilities to prevent, detect, respond to, and recover from attacks involving improvised explosive devices (IEDs) and other non-conventional weapons.

Section 102 of the Maritime Transportation Security Act of 2002, as amended, 46 U.S.C. § 70107, established the PSGP to provide for the establishment of a grant program for making a fair and equitable allocation of funds to implement Area Maritime Transportation Security Plans and facility security plans among port authorities, facility operators, and State and local government agencies required to provide port security services.

Before awarding a grant under the program, the Secretary shall provide for review and comment by the appropriate Federal Maritime Security Coordinators and the Maritime Administrator. In administering the grant program, the Secretary shall take into account national economic and strategic defense concerns based upon the most current risk assessments available.” In addition, any information collected by FEMA for this program is in accordance with 46 U.S.C. § 70107(g), as amended by section 112(c) of the Security and Accountability For Every (SAFE) Port Act of 2006 (Pub .L. No. 109-347), which states: “Any entity subject to an Area Maritime Transportation Security Plan may submit an application for a grant under this section, at such time, in such form, and containing such information and assurances as the Secretary may require.”

Information related to the PSCG is collected as part of OMB ICR No. 1660-0114 from the general public, specifically, State, local, and private organizations requesting federal funds. During the application process, grant applicant’s points-of-contact (POC) and or representatives provide their name, title, address, phone number(s), email address, and signatures. Grant applicants enter PSGP grant information into the FEMA Non-Disaster (ND) Grants Management System which consolidates the entire non-disaster grants management lifecycle into a single system. The FEMA ND Grants system is currently adjudicated by DHS under the FEMA Grant Management Programs PIA and the related DHS/FEMA – 004 Grant Management Information Files SORN.

2. Project or Program status		Existing	
Date first developed:	October 1, 2010	Pilot launch date:	Click here to enter a date.
Date last updated:	October 1, 2010	Pilot end date:	Click here to enter a date.



<p>3. From whom does the Project or Program collect, maintain, use or disseminate information? <i>Please check all that apply.</i></p>	<p><input checked="" type="checkbox"/> DHS Employees</p> <p><input checked="" type="checkbox"/> Contractors working on behalf of DHS</p> <p><input checked="" type="checkbox"/> Members of the public</p> <p><input 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>The PSGP collects the following information about grant applicant's POC or representative:</p> <p>Name;</p> <p>Title/Position;</p> <p>Mailing address(es);</p> <p>Email address(es); and</p> <p>Phone number(s).</p> <p>PSGP may collect the following additional information of applicant employees as part of an applicant's supporting documentation:</p> <p>Name;</p> <p>Title/Position; and</p> <p>Salary (annual).</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</p>	<p><input type="checkbox"/> Closed Circuit Television (CCTV)</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.



Privacy Threshold Analysis

Version date: July 7, 2012

Page 5 of 7

<p>following technologies:</p> <p><i>If project or program utilizes any of these technologies, please contact Component Privacy Officer for specialized PTA.</i></p>	<input type="checkbox"/> Sharepoint-as-a-Service <input type="checkbox"/> Social Media <input type="checkbox"/> Mobile Application (or GPS) <input type="checkbox"/> Web portal ² <input checked="" type="checkbox"/> None of the above
<p>If this project is a technology/system, does it relate solely to infrastructure?</p> <p><i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i></p>	<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.
<p>If header or payload data³ is stored in the communication traffic log, please detail the data elements stored.</p>	
<p>Click here to enter text.</p>	

<p>6. Does this project or program connect, receive, or share PII with any other DHS programs or systems⁴?</p>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: FEMA ND Grants
<p>7. Does this project or program connect, receive, or share PII with any external (non-DHS) partners or systems?</p>	<input type="checkbox"/> No. <input checked="" type="checkbox"/> Yes. If yes, please list: HHS Grants.gov
<p>Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</p>	<p>Choose an item.</p> <p>Please describe applicable information sharing governance in place.</p> <p>Not Applicable</p>

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.”

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:	LeVar J. Sykes
Date submitted to DHS Privacy Office:	July 1, 2013
Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
Recommend coverage by the FEMA Grant Management Programs PIA and the related DHS/FEMA – 004 Grant Management Information Files SORN. Please note that these two documents are currently being reviewed, updated, and possibly renamed.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Jameson Morgan
Date approved by DHS Privacy Office:	August 26, 2013
PCTS Workflow Number:	986420

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.
PIA:	System covered by existing PIA If covered by existing PIA, please list: DHS/FEMA/PIA – 013 Grant Management Programs



Privacy Threshold Analysis

Version date: July 7, 2012

Page 7 of 7

SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/FEMA-004 Grant Management Information Files
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
<p>The DHS Privacy Office concurs with the FEMA Privacy Office's assessment. This system will receive coverage under the DHS/FEMA/PIA – 013 Grant Management Programs PIA and the DHS/FEMA – 004 Grant Management Information Files SORN.</p> <p>The PSGP is one tool used to strengthen the nation's critical infrastructure against risks associated with potential terrorist attacks. PSGP funds support increased protection to critical infrastructure sites. In order to fulfill this mission, the system must collect a minor amount of PII from grant applicants and state points-of-contact (POC) and or representatives such as: name, address, phone number(s), email address, etc.</p> <p>The DHS/FEMA/PIA – 013 Grant Management Programs PIA provides sufficient coverage for the information collection described in this PTA as the purpose of the PIA is to allow for information to be collected in order to determine awards for disaster and non-disaster grants, and for the issuance of awarded funds.</p> <p>The DHS/FEMA – 004 Grant Management Information Files SORN provides coverage to systems of records related to determining awards for disaster and non-disaster grants, and for the issuance of awarded funds. The collection of information in this system is consistent with the purpose, categories of records, and categories of individuals, and routine uses of this SORN.</p>	