

collection of information associated with the DHS complaint form. DHS is proposing to make one change to the DHS compliant form. This change is the addition of a new checkbox that says "gender identity" as a sub-category under the existing checkbox that says "sex" on the form. Gender identity discrimination is a form of sex discrimination, which is covered under Title VII. So this information is already included in data gathered in EEO complaints; adding the separate checkbox just more clearly identifies a sub-category. This form modification is in accordance with new instructions from EEOC—requiring all government agencies to specifically identify this type of information on our complaint forms.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

Analysis

Agency: Office for Civil Rights and Civil Liberties, DHS.

Title: DHS Individual Complaint of Employment Discrimination.

OMB Number: 1610-0001.

Frequency: Annually.

Affected Public: Federal Government.

Number of Respondents: 1200.

Estimated Time per Respondent: 30 minutes.

Total Burden Hours: 600 hours.

Dated: October 9, 2014.

Margaret H. Graves,
Deputy Chief Information Officer.

[FR Doc. 2014-25055 Filed 10-21-14; 8:45 am]

BILLING CODE 9110-9B-P

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: Regional Equipment and Capabilities Exchange, DHS Form 10090 and DHS Form 10089

AGENCY: Domestic Nuclear Detection Office, DHS.

ACTION: 30-Day Notice and request for comments; New Collection, 1601-NEW.

SUMMARY: The Department of Homeland Security, Domestic Nuclear Detection Office, DHS will submit the following information collection request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995 (Pub. L. 104-13, 44 U.S.C. Chapter 35). DHS previously published this information collection request (ICR) in the **Federal Register** on July 1, 2014 at 79 FR 37337 for a 60-day public comment period. No comments were received by DHS. The purpose of this notice is to allow additional 30-days for public comments.

DATES: Comments are encouraged and will be accepted until November 21, 2014. This process is conducted in accordance with 5 CFR 1320.10.

ADDRESSES: Interested persons are invited to submit written comments on the proposed information collection to the Office of Information and Regulatory Affairs, Office of Management and Budget. Comments should be addressed to OMB Desk Officer, Department of Homeland Security and sent via electronic mail to oir_submission@omb.eop.gov or faxed to (202) 395-5806.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

SUPPLEMENTARY INFORMATION: The Joint Analysis Center (JAC), of the Operation Support Division, is responsible for providing awareness of the Global Nuclear Detection Architecture (GNDA), and functions as a central point of the GNDA providing awareness of nuclear threats to the Domestic Nuclear Detection Office (DNDO). The JAC plans to implement a Regional Equipment and Capabilities Exchange (RECE) to identify and compare existing information referencing the domestic nuclear radiological detection capabilities of all participating stakeholders.

The circumstances that make the RECE necessary is the need for a database that accurately reflects the current R/N detection capabilities federal, state, tribal, territorial, and local (FSTTL) stakeholders.

The RECE will recognize a standard process and procedure that the JAC facilitates to ensure a collaborative and coordinated data collection methodology is followed for fidelity of information. The successful implementation of the RECE will aid DNDO in achieving specific objectives mandated in National Security Presidential Directive (NSPD)-43/ Homeland Security Presidential Directive (HSPD)-14, and codified in Title 6, United States Code (U.S.C.) 592. Attached is the HSPD14/NSPD43, please reference the following sections within NSPD-43/HSPD-14:

Subject: Domestic Nuclear Detection

(1)(b) Continue to enhance the effective integration of nuclear and radiological detection capabilities across Federal, State, local, and tribal governments and the private sector for a managed, coordinated response;

(2)(b) Enhance and coordinate the nuclear detection efforts of Federal, State, local, and tribal governments and the private sector to ensure a managed, coordinated response;

(2)(f) Support and enhance the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as provide appropriate information to these entities; and

DNDO needs the information to be collected by the RECE to enhance and coordinate the rad/nuc detection efforts of Federal, State, local and tribal governments, and to effectively share the resources information with all interested entities.

Although not legal justification to collect information, the 2010 GNDA Strategic Plan goals are provided as

additional information that serves as examples for how this collection effort supports internal DNDO initiatives.

The RECE directly relates to the following specific goals within the 2010 GNDA Strategic Plan:

- Goal 3: Communicate—Exchange relevant data, by receiving information from and disseminating information to relevant authorities and the general public, as appropriate.
- Goal 4: Coordinate—Ensure that stakeholders with GNDA functions minimize gaps and unintended overlaps in roles and responsibilities, including through collaboration and cooperation.

Additionally, the RECE helps DNDO meet DHS' lead and supporting roles in the following 2010 GNDA Strategic Plan Objectives:

- Objective 4: Assist state, local, and tribal governments in detecting and reporting on any unauthorized nuclear and radiological materials within their jurisdictions.
- Objective 5: Develop or enhance the federal interior detection architectures and strategies.
- Objective 7: Receive information from, and disseminate information to relevant authorities and the general public.
- Objective 8: Ensure that Stakeholders with GNDA functions minimize gaps and unnecessary overlaps in roles, responsibilities, and activities.
- Objective 9: Ensure that the GNDA can adapt and react in response to changes in technology, protocols, and adversary capabilities.

Information collected is the type used in the ordinary course of business (official business Points of Contact; names, addresses, emails, office phone number to call.) The purpose of the RECE form (DHS Form 10089) is to collect and warehouse relevant data for federal, state, tribal, territorial, and local (FSTTL) authorities to minimize gaps and unintended overlaps in roles and responsibilities for radiological or nuclear (R/N) detection capabilities. The primary purpose of the RECE Questionnaire form is to collect data on current stakeholder (primarily directed at state and local) radiological or nuclear (R/N) detection equipment inventories and resources to streamline access to a real-time depiction of R/N detection capabilities and serve as a warehouse for the data. Data collected will be available via the Joint Analysis Center Collaborative Information System (JACCIS). The Adobe Active "fillable" form focuses on the specific information regarding the respective R/N detection program plans, assets, and status of equipment. As part of the

overall mission of the JAC, the RECE presents an opportunity to extend access to stakeholders with a RND mission, program, or equipment but not reflected in an accessible database.

The JAC aims to provide assistance to State or Local entities with limited access to resources as part of the RECE, and establish a standing collection strategy. Information can be submitted through use of a questionnaire (hard/soft copy transmittal), or scripted phone interviews. The questionnaire will be distributed in compatible file format Adobe PDF Fill-able Form. All emails and phone interviews will not deviate from the scope or content of the DHS Form 10089. Phone interviews will be conducted on an as needed basis for the purposes of non-submittals or to address questions related to answers of information provided within the form.

All data submitted will be processed and stored in a Microsoft Excel spreadsheet for review prior to Joint Analysis Center Collaborative Information System (JACCIS) integration. The RECE will help to accurately reflect the current domestic radiological and detection capabilities within JACCIS. The JACCIS Dashboard provides a secure web interface to collaborate with mission partners and includes a GIS that allows users to view detection information, detectors, situational awareness reports, and other overlays (critical infrastructure, etc.) in a geospatial viewer. Web Service interfaces to other mission partner's systems and content routers provide linkages to detection assets around the country in real-time.

The information collected will be used to provide a more accurate or real-time depiction of the GNDA.

Information can be submitted through use of a questionnaire (hard/soft copy transmittal), email DNDO.JAC2@HQ.DHS.GOV or phone interviews 1-877-363-6522. Use of these three methods of information submittals provides flexibility to the targeted collection audience which may have limited access to technological collection. All data submitted will be processed and stored in an excel spreadsheet, saved in a designated folder within a non-public DHS network share drive folder. Following review of spreadsheet information, data will be integrated into JACCIS in accordance with agreed distribution or sharing regulations; each questionnaire participant will be encouraged to acquire a JACCIS account, and point of contact information for JACCIS account acquisition are included within DHS Form 10089 RECE Questionnaire Directives. Information already available

cannot be used or modified for use because it extremely dated, and lacks the specificity required for accurate accountability. To provide real-time depiction of the GNDA, there needs to be accountability of current resources available at all levels. RND equipment varies greatly between States, Territories and Local jurisdictions, and it is often not controlled or regulated by a single entity.

Efforts to identify duplication have included coordination with Federal stakeholders such as FEMA, CBP, and the FBI; each engagement revealed none of these agencies were in possession of a comprehensive complete data source which included specific domestic (United States) R/N detection capabilities for all States, Territories or Local jurisdictions.

In 2007 and 2009 COL Brent Bredehoff Deputy Assistant Director (in 2007/2009) of the Joint Analysis Center (JAC) directed his staff to conduct an informal information data call to federal entities only. In 2007 State and Local data was collected by the FBI (2006/2007) and provided to the JAC. Neither data collection was for JACCIS, but a plan was developed to put data collected in JACCIS after receiving. This information was neither consistent nor comprehensive and largely inaccurate since much of the information was haphazardly compiled with limited distribution. Additionally the FBI has not updated or made available a revised version of the 2006/2007 data call.

Additionally the RECE is organizing and analyzing relevant data from domestic Preventative Radiological Nuclear Detection (PRND) reports, specifically the National Capabilities Effort (NCE), but many of these NCE reports are extremely dated (greater than 5 years old), do not provide definitive identification details regarding equipment, therefore there is no way to de-conflict with existing equipment data. The NCE reports were a contracted effort through Defense Threat Reduction Agency (DTRA), and due to proprietary limitations when distributed to DNDO were not accompanied by the related raw data collection. Additionally, the NCE reports were created through informal collection techniques, and are largely inconsistent.

Lastly, in the years since the NCE reports and JACCIS informal data calls many States, Territories and Local jurisdictions have made significant advancements and or efforts towards acquiring R/N detection capability. With that said, State, Territories and Local jurisdictions are not subjected to any standing reporting requirement regarding R/N detection equipment or

capabilities, which precludes DNDO or any other Federal Agency from providing a real-time and accurate accountability to decision-makers regarding available domestic R/N detection assets.

There is no assurance of confidentiality provided to respondents. There will be no collection of trade secret or business proprietary information. Furnishing this information is voluntary; however, failure to furnish the requested information may prevent a user from contributing radiological or nuclear detection information to RECE. This could cause a hindrance when attempting to allocate resources during a global nuclear detection architecture related threat incident.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

Analysis

Agency: Domestic Nuclear Detection Office, DHS.

Title: Regional Equipment and Capabilities Exchange.

OMB Number: 1601-NEW.

Frequency: Annually.

Affected Public: State, Local, Tribal Governments.

Number of Respondents: 102.

Estimated Time per Respondent: 1 hour.

Total Burden Hours: 102.

Dated: October 9, 2014.

Margaret H. Graves,

Deputy Chief Information Officer.

[FR Doc. 2014-25050 Filed 10-21-14; 8:45 am]

BILLING CODE 9110-9D-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

United States Secret Service Protective Mission Panel

AGENCY: Office of the Secretary, Department of Homeland Security.

ACTION: Committee management: notice of committee establishment.

SUMMARY: In order to facilitate an effective review of the security provided by the U.S. Secret Service to the White House compound, the Department of Homeland Security (Department or DHS) is creating the U.S. Secret Service Protective Mission Panel (USSSPMP or Panel). Pursuant to the Homeland Security Act of 2002, the Department is taking immediate measures to establish this independent panel of experts to inquire into recent incidents at the White House compound and to provide to the Secretary of Homeland Security recommendations for potential new directors of the U.S. Secret Service and whether there should be a broader review of the U.S. Secret Service.

Name of Committee: U.S. Secret Service Protective Mission Panel.

FOR FURTHER INFORMATION CONTACT: Peter Boogaard, Office of Public Affairs, (202) 282-8010, *MediaInquiry@HQ.DHS.GOV*.

SUPPLEMENTARY INFORMATION:

I. Background

DHS is establishing an independent panel to review the recent fence jumping incident at the White House on September 19, 2014 and related issues concerning security at the White House compound; to provide recommendations for potential new directors of the Secret Service; and to recommend whether there should be a broader review of the Secret Service. This time-sensitive and important review will entail discussion of classified information.

This Department has recognized in the past that some highly critical issues cannot be discussed in public without jeopardizing the security and confidentiality of sensitive homeland security information. For example, in 2006, the Department established the Critical Infrastructure Partnership Advisory Council (CIPAC) to aid in the communication and coordination between critical private sector entities and the Federal agencies charged with regulating them. See 71 FR 14930 (Mar. 24, 2006). Discussions between the members of that Council involve intelligence and law enforcement

information and remain non-public to avoid giving our nation's enemies information they could use to effectively attack a particular infrastructure.

Many of the issues to be reviewed by the Panel will require access to, and discussion of, non-public classified information and other non-public law enforcement sensitive information. These matters include protective measures at the White House, sensitive law enforcement techniques and methods, and the management of these protective and law enforcement missions of the Secret Service.

II. Identifying Solutions

The Department recognizes the importance of the Federal Advisory Committee Act (FACA). The FACA, when it applies, generally requires advisory committees to meet in open session and make publicly available associated written materials. It also requires a 15-day notice before any meeting may be closed to public attendance. These requirements, however, would prevent the Department from convening on short notice a panel to discuss the sensitive and classified information surrounding the review of protective measures at the White House compound and other U.S. Secret Service law enforcement missions in an appropriate setting. The FACA contains a number of exceptions to its general disclosure rules, but the applicability of those exceptions are not sufficient to address the proper handling of classified material and the protection of law enforcement sensitive information in this unique context. The information that will be discussed and reviewed by this panel will be deliberative in nature and will involve classified information that, if discussed in public, would result in the unauthorized disclosure of information that could reasonably be expected to result in threats or damage to national security. Furthermore, the information discussed will involve techniques and procedures for law enforcement investigations. The release of this information would enable criminals and enemies to use that information to circumvent the law and could reasonably be expected to endanger the life or physical safety of individuals.

Section 871 of the Homeland Security Act provides the Secretary of Homeland Security with the authority to establish advisory committees and exempt them from the FACA. 6 U.S.C. 451(a). This authority allows the Department to freely and completely review the security procedures, to discuss potential vulnerabilities, and to provide the Department with information and