program participants (including recipients, borrowers, grantees, and contractors), USDA employees, and other USDA information. RADAR will also contain records OIG ODS generates that are the result of its data analysis and data analytics work.

RECORD SOURCE CATEGORIES:

Information contained in this system is obtained from systems of records maintained by USDA and other Government agencies; individuals; non-Government, commercial, public, and private agencies and organizations; media, including periodicals, newspapers, and broadcast transcripts; and publicly-available databases.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSE OF SUCH USES:

Routine Uses 1 through 16, 19, 20, and 21 apply. 80 FR 48476 (Aug. 13, 2015).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The RADAR System, USDA/OIG–8, consists of computerized and paper records.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

The records are retrieved by names, addresses, Social Security Numbers, and tax identification numbers of USDA program participants or employees, or by case numbers. Records are retrieved by USDA OIG's Office of Data Sciences employees.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records contained in this system are currently unscheduled. A record retention schedule will be developed and submitted to NARA for approval. No records will be destroyed until a NARA approved record retention schedule is in place.

Any records contained in the system before the creation of the Office of Data Sciences, are retained and disposed of in compliance with OIG's record disposition authority approved by NARA for Inspector General Audit and Evaluation Case Files.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

OIG has adopted appropriate administrative, technical, and physical controls in accordance with OIG's information security policies to protect the security, integrity, and availability of the information, and to ensure that records are not disclosed to or accessed by unauthorized individuals.

Computerized records are maintained in a secure, password protected computer system. The computer server is maintained in a secure, access-controlled area within an access-controlled building. Paper records are kept in limited access areas during duty hours and in locked offices during nonduty hours.

RECORD ACCESS PROCEDURES:

An individual may request access to a record in this system that pertains to him/her by submitting a written request to the Counsel to the Inspector General, Office of Inspector General, U.S. Department of Agriculture, 1400 Independence Avenue SW., Stop 2308, Washington, DC 20250–2308.

CONTESTING RECORD PROCEDURES:

An individual may contest information in this system that pertains to him/her by submitting a written request to the Counsel to the Inspector General, Office of Inspector General, U.S. Department of Agriculture, 1400 Independence Avenue SW., Stop 2308, Washington, DC 20250–2308. This system may contain records originated by USDA agencies and contained in USDA's other systems of records. Where appropriate, coordination will be effected with the appropriate USDA agency regarding individuals contesting records in the relevant system of records.

NOTIFICATION PROCEDURES:

Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her, from the Counsel to the Inspector General, Office of Inspector General, U.S. Department of Agriculture, 1400 Independence Avenue SW., Stop 2308, Washington, DC 20250–2308.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

No exemptions are applicable to records created by OIG ODS in the RADAR System, USDA/OIG–8. For individual records originating within a USDA system of records, OIG will continue to apply any applicable Privacy Act exemptions to those individual records.

HISTORY:

USDA OIG updated and published its system of records notices in their entirety on August 13, 2015. 80 FR 48476. System of Records USDA/OIG–8, originally established on March 5, 2009 (74 FR 9584), was included and updated in that consolidated notice.

[FR Doc. 2017–01412 Filed 1–19–17; 8:45 am]

BILLING CODE 3410–23–P

DEPARTMENT OF COMMERCE

Submission for OMB Review; Comment Request Information Collection for Self-Certification to the EU-U.S. Privacy Shield Framework

The Department of Commerce will submit to the Office of Management and Budget (OMB) for clearance the following proposal for collection of information under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35).

Agency: International Trade Administration (ITA).

Title: Information Collection for Self-Certification to the EU-U.S. Privacy Shield Framework.

OMB Control Number: 0625–0276.

Form Number(s): None.

Type of Request: Regular submission.

Number of Respondents: 3,600.

Average Hours per Response: 38 minutes.

Burden Hours: 2,954.

Needs and Uses: The United States and the European Union (EU) share the goal of enhancing privacy protection for their citizens, but take different approaches to protecting personal data. Given those differences, the Department of Commerce (DOC) developed the EU-U.S. Privacy Shield Framework (Privacy Shield) in consultation with the European Commission, as well as with industry and other stakeholders, to provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from the European Union while ensuring the protection of the data as required by EU law.

On July 12, 2016, the European Commission deemed the Privacy Shield Framework adequate to enable data transfers under EU law, and the DOC began accepting self-certification submissions from organizations on August 1, 2016. More information on the Privacy Shield is available at: *https://www.privacyshield.gov/welcome*.

The DOC has issued the Privacy Shield Principles under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. 1512). The International Trade Administration (ITA) administers and supervises the Privacy Shield, including by maintaining and making publicly available an authoritative list of U.S. organizations that have self-certified to the DOC. U.S. organizations submit information to ITA to self-certify their compliance with Privacy Shield.

U.S. organizations considering self-certifying to the Privacy Shield should review the Privacy Shield Framework.

In summary, in order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC), the Department of Transportation, or another statutory body that will effectively ensure compliance with the Principles; (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with the Principles; and (d) fully implement them.

Self-certification to the DOC is voluntary; however, an organization's failure to comply with the Principles after its self-certification is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. 45(a)) or other laws or regulations prohibiting such acts.

In order to rely on the Privacy Shield for transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the DOC, be placed by ITA on the Privacy Shield List, and remain on the Privacy Shield List. To self-certify for the Privacy Shield, an organization must provide to the DOC a self-certification submission that contains the information specified in the Privacy Shield Principles. The Privacy Shield self-certification form would be the means by which an organization would provide the relevant information to ITA.

ITA has committed to follow up with organizations that have been removed from the Privacy Shield List. ITA will send questionnaires to organizations that fail to complete the annual certification or who have withdrawn from the Privacy Shield to verify whether they will return, delete, or continue to apply the Principles to the personal information that they received while they participated in the Privacy Shield, and if personal information will be retained, verify who within the organization will serve as an ongoing point of contact for Privacy Shield-related questions.

In addition, ITA has committed to conduct compliance reviews on an ongoing basis, including through sending detailed questionnaires to participating organizations. In particular, such compliance reviews shall take place when: (a) The DOC has received specific non-frivolous complaints about an organization's compliance with the Principles, (b) an organization does not respond satisfactorily to inquiries by the DOC for information relating to the Privacy Shield, or (c) there is credible evidence that an organization does not comply with its commitments under the Privacy Shield.

Affected Public: Primarily businesses or other for-profit organizations.

Frequency: Annual and periodic.

Respondent's Obligation: Voluntary.

This information collection request may be viewed at *www.reginfo.gov.* Follow the instructions to view the Department of Commerce collections currently under review by OMB.

Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to OIRA *Submission@omb.eop.gov* or fax to (202) 975–5806.

Sheleen Dumas,

PRA Departmental Lead, Office of the Chief Information Officer.

[FR Doc. 2017–01334 Filed 1–19–17; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

Information Systems Technical Advisory Committee; Notice of Partially Closed Meeting

The Information Systems Technical Advisory Committee (ISTAC) will meet on January 25 and 26, 2017, 9:00 a.m., in the Herbert C. Hoover Building, Room 3884, 14th Street between Constitution and Pennsylvania Avenues NW., Washington, DC. The Committee advises the Office of the Assistant Secretary for Export Administration on technical questions that affect the level of export controls applicable to information systems equipment and technology.

Wednesday, January 25

Open Session

1. Welcome and Introductions
2. Working Group Reports
3. Old Business
4. Industry Presentations: Quantum Computing
5. New business

Thursday, January 26

Closed Session

6. Discussion of matters determined to be exempt from the provisions relating to public meetings found in 5 U.S.C. app. 2 §§ 10(a)(1) and 10(a)(3).

The open session will be accessible via teleconference to 20 participants on a first come, first serve basis. To join the conference, submit inquiries to Ms. Yvette Springer at *Yvette.Springer@bis.doc.gov,* no later than January 18, 2017.

A limited number of seats will be available for the public session. Reservations are not accepted. To the extent time permits, members of the public may present oral statements to the Committee. The public may submit written statements at any time before or after the meeting. However, to facilitate distribution of public presentation materials to Committee members, the Committee suggests that public presentation materials or comments be forwarded before the meeting to Ms. Springer.

The Assistant Secretary for Administration, with the concurrence of the delegate of the General Counsel, formally determined on January 12, 2017, pursuant to Section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. app. 2 § 10(d)), that the portion of the meeting concerning trade secrets and commercial or financial information deemed privileged or confidential as described in 5 U.S.C. 552b(c)(4) and the portion of the meeting concerning matters the disclosure of which would be likely to frustrate significantly implementation of an agency action as described in 5 U.S.C. 552b(c)(9)(B) shall be exempt from the provisions relating to public meetings found in 5 U.S.C. app. 2 §§ 10(a)(1) and 10(a)(3). The remaining portions of the meeting will be open to the public.

For more information, call Yvette Springer at (202) 482–2813.

Dated: January 17, 2017.

Yvette Springer,

Committee Liaison Officer.

[FR Doc. 2017–01423 Filed 1–19–17; 8:45 am]

BILLING CODE 3510–JT–P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

Sensors and Instrumentation Technical Advisory Committee; Notice of Partially Closed Meeting

The Sensors and Instrumentation Technical Advisory Committee (SITAC) will meet on February 1, 2017, 9:30 a.m., (Pacific Standard Time) at the SPIE Photonics West, The Moscone Center South, 747 Howard Street, Room 102 South Hall (Exhibit Level), San Francisco, CA 94103. Registration for an exhibit-only pass is required and is available for free. Attendees can register for an exhibit-only pass in advance at *https://spie.org/conferences-and-exhibitions/photonics-west/registration* or sign up onsite at the registration booth. The Committee advises the Office of the Assistant Secretary for Export