PRIVACY IMPACT ASSESSMENT (PIA)

For the

DISA Google Pilot/Authentication Gateway Service (AGS) Cooperative Research and Development Agreement (CRADA)
Defense Information Systems Agency

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☐ **Existing DoD Information System**
- ☒ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☐ **Yes, DITPR** Enter DITPR System Identification Number
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number
- ☒ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier K890.14 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

The authority allows DISA Google Pilot to collect the following data:

- 5 U.S.C. 301, Departmental Regulation;
- DoD Directive 5105.19, Defense Information Systems Agency (DISA);
- DoD Chief Information Officer Memorandum for Director, Defense Information Systems Agency (DISA)

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

DISA will conduct a pilot assessment of identified Google Apps for Government (GAfG) core applications (i.e. Gmail, Contacts, Calendar, Docs, Sheets, Slides) with a limited community of DISA-JITC users. The intent of this pilot is to determine if GafG commercial cloud services and applications can become a cost-effective alternative to similar Enterprise Services and validate next-generation approaches to cloud-based email that can augment Defense Enterprise Email (DEE) service. DISA will also determine if the ESD Authentication Gateway Service (AGS) will provide a CAC proxy authentication solution for DoD users to securely and consistently interface with the Google cloud, DoD domain, and Google applications that are incapable of direct PKI. GAfG will consolidate authoritative personnel identity data from Enterprise Email Global Address List (GALs) integrating it into a single directory. Data collected by DISA may include: Individual's name (last name, first name, middle initial); unique identifiers including Department of Defense Identification number (DoD ID), login name, legacy login name, and personal user name; alias; rank; title; job title; primary and other work e-mail addresses; personal display name (PDN); work contact information, including administrative organization, duty organization, department, company (derived), building, address, mailing address, country, organization, phone, fax, mobile, pager, Defense Switched Network (DSN) phone.

Google does not require all of aforementioned data to create user accounts. However, DISA may leverage leverage this data from existing services, such as the DoD Identity Synchronization Services (IdSS) to acquire the user identities for the authentication gateway.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The PII being collected is low impact PII. This information does not provide an item, collection, or grouping of information in electronic form maintained by a DoD Component that associates personal information such as education, financial transactions, medical history, criminal or employment history, with an individual identifier. It only provides contact information and current employment information (e.g., their position within the organizational structure)

Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal government personnel. Defense-in-Depth methodology is used to protect the repository and interfaces, including (but not limited to) multi-layered firewalls, Secure Sockets Layer/Transport Layer Security connections, directory access control lists, file system permissions, intrusion detection and prevention systems and log monitoring. Complete access to all records is restricted to and controlled by certified system management personnel, who are responsible for maintaining the system integrity and the data confidentiality.

Google access and use to type and amount and management of risk are contained in their privacy policy located at http://www.google.com/policies/privacy/, July 27, 2012.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Defense Information Systems Agency

☒ **Other DoD Components.**

Specify. For DoD white pages and email Global Address Lists (GAL)

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Google

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals may object to the collection of PII by not providing the requested information, however, this information is required to gain access to the network. It will be stressed that the information only provides contact information and current employment information (e.g., their position within the organizational structure).

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Individuals are provided a consent form and they may choose not to sign it, however, this consent is required to gain access to the network. It will be stressed that the information only provides contact information and current employment information (e.g., their position within the organizational structure).

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

PRIVACY ACT STATEMENT

Authority for maintenance of system: 5 U.S.C. 301, Departmental Regulation; DoD Directive 5105.19, Defense Information Systems Agency (DISA).

Purpose(s): Form is used to establish Google for Google Apps account. The DoD Blanket Routine Uses published at the beginning of the DISA's compilation of systems of records notices apply to this system. In addition to those disclosures generally permitted under 5 USC 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside of DoD as a routine use pursuant 5 USC 552a(b)(3) as follows: The 'Blanket Routine uses' set forth at the beginning of the DISA's compilation of systems of records notices apply to this system.

Disclosure: Voluntary; however, failure to provide the information may impede access to the GAfG commercial cloud services and pilot assessment.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.