PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Global Content Delivery Service (GCDS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

GCDS Single Sign-On (SSO)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☒ From Federal employees and/or Federal contractors
- ☐ From both members of the general public and Federal employees and/or Federal contractors
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

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

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

The Global Content Delivery Service (GCDS) is a type-accredited DISA enterprise managed service which provides performance, security, and infrastructure reduction to its DoD mission partners. For over a decade, it has helped the DODIN scale to meet its application and infrastructure challenges by operating a powerful multi-tenant and fully managed web fabric. GCDS is based on the same technology which powers the Akamai commercial platform and that delivers and secures commercial TLS applications for a broad range of industries, including the DoD, U.S. Federal Government, Fortune 500 companies, major banks, retailers, and governments around the world.

The GCDS Managed service is comprised of content delivery, security, and single sign on (SSO) components. For the SSO service, user attributes are retrieved as part of the authentication process from mission owner's controlled and external C/C/S/A identity management systems. These sources exist outside of the GCDS boundary and are not controlled by GCDS; therefore, the potential remains for records to contain PII. The retrieved attributes from the mission owners identity management systems are used to verify the identity of the requester and sent to the mission owner's server infrastructure for further processing (e.g. authorization).

The GCDS SSO service potentially has access to PII data during the collection, use, processing, and disclosure phases. PII is not directly collected by GCDS SSO, however data may flow through GCDS systems in an encrypted form while it is being collected by a system of record. Use and processing of PII data by the GCDS SSO system is limited to making decisions about authentication and authorization, and data is examined in a programmatic way by the system in order to evaluate rules defined by the information owner to allow or disallow access, then user data is discarded. Finally, user data, which may include PII data, is packaged and passed to individual missions when explicitly configured to do so by the information owner. This data is signed and encrypted in transit to protect accidental disclosure to uninvolved third parties.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

GCDS SSO service does not collect PII from individuals and may use PII data received by the dependency identity management system for authentication and authorization decisions. As a result, GCDS SSO will only package the records (including PII data) for use by dependent applications only when explicitly configured to do so.

The GCDS SSO service does not collect PII from individuals and may transport PII data from downstream and dependent customer systems only when configured by customers to support the mission objective. The transport of this PII data is authorized by the customer on a case by case basis, and it is required that each individual mission has completed their own PIA which details the specific use of their PII data.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Data is maintained and stored within information systems outside of GCDS SSO boundary and owned by respectful mission owners; therefore, individuals cannot object to the use of PII attributes that may be used by GCDS SSO as transport and would have to raise objections with the corresponding mission owner's to exclude attributes within their external system (e.g. identity management service). The GCDS SSO service does not add any new PII attributes to the individual's data record as it reads (only) from the dependent and downstream systems, such as the identity management system.

Per section M of this assessment, the USARMY and USAF customers have executed statutory authorities for collecting and maintaining the system of records; further details on how PII is asked (if at all) are handled by the USARMY and USAF.

f. 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.

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

Individual end-users cannot consent to specific use of PII attributes that may be used with the GCDS SSO service; however individuals may be able to specifically-consent with the originating identity management service (downstream of GCDS SSO) to honor any usage of PII attributes.

Per section M of this assessment, the USARMY and USAF customers have executed statutory authorities for collecting and maintaining the system of records; further details on how PII is asked (if at all) are handled by the USARMY and USAF.

The GCDS SSO service will not modify any PII attributes to the individual's data record that do not exist and are accessible via the dependency identity management system.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

Individuals are not asked to provide PII data via the GCDS SSO service. All data available to the GCDS SSO service, including any PII data, exists within the dependency identity management system or web content management system. Any information provided to the user regarding the use of their PII data would originate with that dependency identity management system and any policies or procedures in use that govern the initial collection of user data."

Per section M of this assessment, the USARMY and USAF customers have executed statutory authorities for collecting and maintaining the system of records; further details on how PII is asked (if at all) are handled by the USARMY and USAF.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	DISA; owner of the GCDS managed service
☒ Other DoD Components	Specify.	USARMY EAMS-A, USAF CCE; see statutory authorities for both components
☐ Other Federal Agencies	Specify.	
☐ State and Local Agencies	Specify.	
☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Akamai Technologies cleared employees working on GCDS program supporting the SSO service for USARMY EAMS-A and USAF CCE
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☐ Individuals ☐ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

Source of PII is collected from external USARMY and USAF information systems (identity management for SSO) integrated with GCDS platform, where customers maintain and store the PII outside of the GCDS SSO accreditation boundary.

Per section M of this assessment, the USARMY and USAF customers have executed statutory authorities for collecting and maintaining the system of records; further details on how PII is asked (if at all) are handled by the USARMY and USAF.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] Official Form (*Enter Form Number(s) in the box below*)
- [ ] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [x] Information Sharing - System to System
- [ ] Website/E-Form
- [ ] Other *(If Other, enter the information in the box below)*

k. 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 must be consistent.

- [ ] Yes
- [x] No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

Based on the SORN requirements, GCDS has not been applicable to date, because GCDS does not maintain records and only collects data as transport from mission owner's systems; furthermore, GCDS does not allow for records to be retrieved by a personal identifier.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N/A

(2) If pending, provide the date the SF-115 was submitted to NARA. N/A

(3) Retention Instructions.

N/A

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

Based on the SORN requirements, GCDS has not been applicable to date, because GCDS does not maintain records and only collects data as transport from mission owner's systems; furthermore, GCDS does not allow for records to be retrieved by a personal identifier.

The two GCDS SSO service consumers, USAF CCE and USARMY EAMS-A, have applicable statutory authority for collecting and maintaining a system of records. The executive order numbers for both USAF CCE and USARMY EAMS-A are:
- USAF CCE: 9397
- USARMY EAMS-A: available upon request

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.