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:

USAFRICOM Global Command & Control System (GCCS) - Joint (GCCS-J) HQ, HQ ALT (Del Din), and CJTF-HOA

2. DOD COMPONENT NAME:

United States Africa Command

3. PIA APPROVAL DATE:

02/10/22

USAFRICOM

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [ ] from both members of the general public and Federal employees
- [x] 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.

GCCS-J is the Nation's system of record for the command and control of joint and coalition forces. It incorporates the force planning and readiness assessment applications required by battlefield commanders to effectively plan and execute military operations. Its common operational picture (COP) correlates and fuses data from multiple sensors and intelligence sources to provide war-fighters the situational awareness needed to act and react decisively. It also provides an extensive suite of integrated office automation, messaging, and collaborative applications. GCCS-J is a IS Major application that consists of both Commercial off-the-shelf (COTS)and Government off-the-shelf (GOTS) software. GCCS-J resides on U.S. Africa Command (USAFRICOM) Enterprise Network (AEN)-Secret Internet Protocol Router Network (SIPRNet) also known as AEN-S. GCCS-J only interfaces with other instances of GCCS-J that are configured within the GCCS-J servers / firewall to provide situational awareness, support for intelligence, force planning, readiness assessment, and deployment applications that battlefield commanders require to effectively plan and execute joint military operations. Collected geographical information is compiled and displays a map of a specific area within the USAFRICOM Area of Responsibility (AOR) with landmarks / Points of Interest and is updated constantly with newly received geographical information.

Personnel who require access to GCCS-J are requesting access to AEN-S and providing Agile Client permissions and Active Directory groups that provide access to GCCS-J . The process is initiated on the AEN-Nonclassified Internet Protocol Router Network (NIPRNet), also known as AEN-N, by submitting a DD Form 2875, System Access Authorization Request (SAAR). The information required to complete the Form 2875 is covered in Section 2 of this PIA. The initiator (requester) will submit the DD2875 for review and account creation. The DD2875 is routed to their supervisor or sponsor who validates the requirement for access to AEN-S. The requesters supervisor or sponsor will contact the appropriate Security Manager (SM) and submit the DD2875 to the SM for clearance verification. The SM contacts the requester, via Voice Over Internet Protocol (VOIP) telephone, for their SSN. Once provided/verified the security verification program is cleared to include collected SSN. The SM will verify that the individual has the appropriate clearance for the access requested. The SM will then update the DD2875 account form with the user's clearance information and forward to the Account Service Desk (ASD) for account review/creation. Once an account is created, the initiator is required set up their digital signature. To do this, the individual will report to the ASD offices for visual ID verification, to read the USAFRICOM Acceptable Use User Agreement (AUP), and will complete the DD 2842, PKI Token Request form. At that point, the requester will digitally sign the USAFRICOM account form. ASD will then provide the individual with access to AEN-S. The 2875 itself is processed on AEN-N.

Once access is provided to AEN-S, the individual is provided a smart card with an embedded token that is associated with that individual's Electronic Data Interchange Personal Identifier (EDIPI), also called the DoD ID number. Once the token has been issued, the individual must then choose a personal identification number (PIN) that will be associated with that token in order to access AEN-S. This information is registered in AEN-S and will be recorded each time the individual accesses AEN-S. This token is also used to authenticate, via Agile Client/ Agile Client Server (ACLSVR), to GCCS-J by pulling the certificate chain and validating that ACLSVR trusts the chain, that the client can

properly sign forms with it, and that nothing in the chain has been revoked via Certificate Revocation List (CRL). The EDIPI number is not referenced.

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)*

No PII is collected. GCCS-J does not utilize the EDIPI. GCCS-J authenticates personnel by pulling the certificate chain and validates that ACLSVR trusts the chain, that the client can properly sign forms with it, and that nothing in the chain has been revoked via CRL.

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.

No PII is collected. DD Form 2875 is utilized for access to AEN-S, not GCCS-J. GCCS-J authenticates personnel by pulling the certificate chain and validates that ACLSVR trusts the chain, that the client can properly sign forms with it, and that nothing in the chain has been revoked via CRL. The EDIPI number is not referenced.

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.

No PII is collected. DD Form 2875 is utilized for access to AEN-S, not GCCS-J. GCCS-J authenticates personnel by pulling the certificate chain and validates that ACLSVR trusts the chain, that the client can properly sign forms with it, and that nothing in the chain has been revoked via CRL. The EDIPI number is not referenced.

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

No PII is collected. DD Form 2875 is utilized for access to AEN-S, not GCCS-J. GCCS-J authenticates personnel by pulling the certificate chain and validates that ACLSVR trusts the chain, that the client can properly sign forms with it, and that nothing in the chain has been revoked via CRL. The EDIPI number is not referenced.

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

☒ Within the DoD Component	Specify.	USAFRICOM Account Service Desk
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	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.	
☐ 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

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

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

Note DD Form 2875is used for access to AEN-S, access verification, identification, and authentication only. It is not used to authenticate to GCCS-J. GCCS-J authenticates personnel by pulling the certificate chain and validates that ACLSVR trusts the chain, that the client can properly sign forms with it, and that nothing in the chain has been revoked via CRL. The use of PII for access to AEN-S is covered by a separate PIA for the AEN-S.

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.

PII is not collected on GCCS-J. Authentication and/or Audit data is collected on AEN-S. AEN-S has a separate PIA which lays out its collection, use, and sharing of PII.

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. CJCSM 5760.01A Vol. II

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

(3) Retention Instructions.

0300-04 S - Country studies and/or reports prepared by Defense Intelligence Agency and/or the United States Intelligence Community, consisting of: specialized intelligence publications, estimates, studies, surveys, reports, analyses, evaluations, and appraisals including both general and technical intelligence and intelligence concerning combat applications maintained by any JS/CCMD activity. Destroy when superseded or obsolete.

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.

Although PII is collected as a part of the account creation process, No PII is collected by GCCS-J. Authentication and/or Audit data is collected on AEN-S. AEN-S has a separate PIA which lays out its collection, use, and sharing of PII.

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.

AEN-S does not collect information from members of the public.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

☐ Biometrics	☐ Birth Date	☐ Child Information
☐ Citizenship	☐ Disability Information	☒ DoD ID Number
☐ Driver's License	☐ Education Information	☐ Emergency Contact
☐ Employment Information	☐ Financial Information	☐ Gender/Gender Identification
☐ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☐ Mailing/Home Address	☐ Marital Status	☐ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☒ Official Duty Address	☒ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☐ Personal E-mail Address	☐ Photo
☐ Place of Birth	☒ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☒ Rank/Grade	☐ Religious Preference
☐ Records	☒ Security Information	☐ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☐ If Other, enter the information in the box below	

** NOTE** All of the above checked items are part of DD form 2875 for requesting access to AEN-S, not GCCS-J. See the AEN-S PIA for more information about the collection, use, dissemination of PII for access to the AEN-S.

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☒ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

The GCCS-J does not collect or use the SSNs of individuals for any purpose.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

N/A

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

This section does not apply to the GCCS-J.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

The GCCS-J does not collect or use the SSNs of individuals for any purpose.

b. What is the PII confidentiality impact level[2]? ☒ Low ☐ Moderate ☐ High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically

conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [X] Cipher Locks
- [X] Combination Locks
- [X] Key Cards
- [X] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [X] Identification Badges
- [X] Safes
- [ ] If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- [X] Backups Secured Off-site
- [X] Encryption of Backups
- [X] Methods to Ensure Only Authorized Personnel Access to PII
- [X] Periodic Security Audits
- [X] Regular Monitoring of Users' Security Practices
- [X] If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [X] Encryption of Data at Rest
- [X] Firewall
- [X] Role-Based Access Controls
- [X] Virtual Private Network (VPN)
- [ ] Common Access Card (CAC)
- [X] Encryption of Data in Transit
- [X] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [X] If Other, enter the information in the box below
- [X] DoD Public Key Infrastructure Certificates
- [ ] External Certificate Authority Certificates
- [X] Least Privilege Access
- [X] User Identification and Password

The following technical controls are managed at an Enterprise level by USAFRICOM J6:
1. Encryption of Data at Rest - USAFRICOM employs full-disk encryption mechanisms to ensure that PII data-at-rest is protected from intentional or accidental disclosure or loss.
2. Firewall - USAFRICOM employs firewall border control mechanisms that restrict access to PII data stored internally on the AEN-S. Firewall rules prevent exposure of USAFRICOM managed PII to the outside world.
3. Role-Based Access Controls - The AEN-S utilizes Microsoft Active Directory to manage user access to internal network resources. Users and groups of users are allowed access to PII data where the information owner grants access on the basis of need-to-know.
4. SIPR Token- The AEN-S utilizes the DOD SIPR Token system to manage user access to USAFRICOM IT assets. Token issuance is contingent upon background vetting and user job role.
5. Encryption of Data in Transit - Through the use of the DOD SIPR Token, each user is enabled to encrypt email through DOD SIPR Token mechanisms.
6. Intrusion Detection Systems (IDS) - USAFRICOM AEN-S is guarded by IDS systems that enable Cybersecurity professionals the ability to find and stop intrusions into the network.
7. Least Privilege Access - The AEN-S applies the principle of least privilege in its management of network accounts as well as in the granting of access to network resources containing PII information.
8. User Identification and Password - This technical capability is limited to the greatest extent possible with DOD SIPR Tokens required to access network resources wherever possible. In the rare instances where this capability is applied, DOD complexity requirements for passwords are enforced through Enterprise Active Directory control mechanisms. Secret Internet Protocol Router Network (SIPRNet) Token
9. Vulnerability Management - In accordance with USCYBERCOM TASKORD 17-0019. FRAGO 1 to TASKORD 17-0019, JFHQ-DODIN CTO 20-0020 and the DISA ACAS Best Practice Guide, The Assured Compliance Assessment Solution is the DoD mandated Vulnerability Scanning tool for USAFRCIOM Information Systems. The tool is utilized for required Weekly Vulnerability Scanning, STIG Configuration, and Network Vulnerability Monitoring.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Complete access to all records is restricted to and controlled by the data owner who is responsible for maintaining data integrity and