

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:

United States Africa Command Enterprise Network (AEN) Secret Internet Protocol Router Network (SIPRNET) (AEN-S)

2. DOD COMPONENT NAME:

United States Africa Command

3. PIA APPROVAL DATE:

04/21/21

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

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.

Secret Internet Protocol Router Network (SIPRNet) is the SECRET component of the Defense Information Systems Network which combines infrastructure components such as routers, switches, and servers. USAFRICOM Enterprise Network SIPRnet (AEN-S) is the USAFRICOM instance of the SIPRNet. It is a computer network used by USAFRICOM to transmit classified information (up to and including information classified SECRET) by packet switching over a secure environment. AEN-S provides a network-computing that lessens the number of systems and amount of information exposed to snooping, compromise, and theft from sources both within and outside of AEN-S through implementation of this system security design. AEN-S supports local area network (LAN) and wide area network (WAN) connectivity. It provides the mechanism for AEN-S users to communicate via the Transmission Control Protocol/Internet Protocol (TCP/IP) over Ethernet. AEN-S provides a network computing environment for all USAFRICOM users who need access to an environment that has been approved to transmit and maintain information classified at the secret level. All USAFRICOM Offices and Directorates have access to the AEN-S, but access is only provided to those with the need to access information classified at the SECRET level.

Users who require access to AEN-S must initiate the process by submitting a DD Form 2875, System Access Authorization Request (SAAR), via INFOPATH, a Microsoft product which enables electronic generation of forms, is used to create an electronic 2875 account request form. The initiator will submit the form to Microsoft Workflows process and task automation tool to route the form to the appropriate approving personnel and to the AFRICOM Service Desk (ASD) for review and account creation. The form is routed to the requestor (the initiator's supervisor or sponsor), who validates the requirement for access to AEN-S and the type of account the initiator requires. The requestor must also contact the initiator's Security Manager (SM) and submit the DD 2875 to the SM for clearance verification. Once the form has been submitted, the SM will receive notification from Workflows of the new request. The SM will then access the form in their Workflows dashboard. The SM verify that the individual has the appropriate clearance for the access requested. They will, then, update the AFRICOM account form with the user's clearance, and submit the DD2875 via Workflows to the USAFRICOM Service Desk (ASD) for review and account creation. Once an account is created, initiator is required set up their digital signature. To do this, the individual will report to the ASD offices for visual ID verification, read the USAFRICOM Acceptable Use User Agreement (AUP), and the DD 2842, PKI Token Request forms. At that point, they will digitally sign the USAFRICOM account form. ASD will then provide the individual with access to AEN-S.

Once access is provided, the individual is provided a smart card with an embedded token that is associated with that individual's 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 provide access to AEN-S. This information is registered in AEN-S and will be recorded each time the individual accesses AEN-S.

Once users are provided access to AEN-S, they are able to access e-mail and web services.

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)

The AEN-S system does not collect or store PII. However, is a platform that supports underlying systems and applications that may collect PII. PII that is stored on AEN-S may be collected and used by USAFRICOM components for a variety of reasons. The individual organizations that store information on the AES will complete PIAs that document their collection and use of PII. Audit and access records, when accessing / utilizing AEN-S contain only the individual's DoD ID number, which is not associated with any other PII.

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.

An individual's opportunity to object to collection of their PII is when submitting the account form or during their requisite background investigation. The access information was submitted to verify that the initiator possesses the requisite clearance level for access to AEN-S. AEN-S collects only the individual's DOD ID number. The platform does not collect or maintain any other PII.

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.

An individual's opportunity to object to specific uses of PII is during their background investigation, or when submitting the account form to request system access. While applications and services found on the AEN-S may collect, use, and disseminate PII, the AEN itself does not collect or maintain user PII other than the DoD ID number of the individuals who access it.

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

Once an individual is provided access to AEN-S, the system does not associate the DOD-ID number with any other information. The only time that the DOD-ID would be reassociated with other identifiers is if misconduct is detected while using the system. This information is not available within the AEN-S and is never entered into the system.

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.

All AFRICOM Offices and Directorates have access to the AEN-S.

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

To gain access to AEN-S, users must submit a DD Form 2875, System Access Authorization Request (SAAR), however AEN-S does not

collect or maintain PII

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

- | | |
|--|--|
| <input type="checkbox"/> E-mail | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input checked="" type="checkbox"/> In-Person Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input type="checkbox"/> Information Sharing - System to System | <input checked="" type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other: (If Other, enter the information in the box below) | |

In order for access to be granted to the AEN-S, PII is collected via the DD Form 2875. The PII that is collected via the DD 2875 is used for identity verification. In addition, the individual must show their Common Access Card to ASD personnel for purposes of identity verification before establishing their digital signature.

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 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.

Although the DD 2875 is used to verify and validate users who request access to the AEN-S. The AEN-S only collects the individual's Electronic Data Interchange Personnel Identifier (EDIPI), also known as the DoD identification (ID) number, for access and audit purposes.

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.

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

(3) Retention Instructions:

Systems requiring special accountability for access. These are user identification records associated with systems which are highly sensitive and potentially vulnerable. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

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 statute 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.

10 U.S.C § 113 10 U.S.C. § 164, Commanders of Combatant Commands; Executive Order (E.O.)10450, E.O. 9397, as amended; and Public Law 99-474, the Computer Fraud and Abuse Act.

NOTE: Authorities for subsystems of AEN-S are not included here. Those subsystems will provide their authorities to collect information via their own, individual PIAs.

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.

USAFRICOM AEN-S does not collect information directly from 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)

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

though the above information is collected in order to grant access to AEN-S, AEN-S collects only information pertaining to audit and access. AEN-S access and audit records collect and use only the DoD ID number.

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.

Neither the AEN-S registration process, nor the audit and access features collect or use SSNs 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".

The AEN-S does not collect or use SSNs for any purpose.

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

This section does not apply to the AEN-S, as no part of the registration process uses the SSN. While subsystems found on the AEN-S platform may collect use and/or disseminate the SSN, AEN-S does not collect, maintain, or disseminate SSNs.

(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

As stated above, the AEN-S does not collect or use the SSNs of individuals for any purpose.

b. What is the PII confidentiality impact level²? Low Moderate High

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

²Guidance 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

c. How will the PII be secured?

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

- | | |
|---|---|
| <input checked="" type="checkbox"/> Cipher Locks | <input type="checkbox"/> Closed Circuit TV (CCTV) |
| <input checked="" type="checkbox"/> Combination Locks | <input checked="" type="checkbox"/> Identification Badges |
| <input checked="" type="checkbox"/> Key Cards | <input checked="" type="checkbox"/> Safes |
| <input checked="" type="checkbox"/> Security Guards | <input type="checkbox"/> If Other, enter the information in the box below |

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

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

PII holdings will be reviewed at a minimum annually to ensure the PII stored is still required.

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

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

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.
8. 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.
9. 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
10. Websites -
11. HBSS -
12. 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 USAFRICOM 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 are responsible for maintaining data integrity and confidentiality.