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:			3. PIA APPROVAL DATE:	
United States Africa Command			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		
X 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 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.

	(hy is the PII collected and/or what is the intended use of the PII? (e. dministrative use)	.g., verific	ation, identification, authentication, data matching, mission-related 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	o individuals have the opportunity to object to the collection of their	PII?	Yes X No	
(1)	If "Yes," describe the method by which individuals can object to the collec	tion of P	1.	
(2)	If "No," state the reason why individuals cannot object to the collection of	PII.		
inves	ndividual's opportunity to object to collection of their PII is when stigation. The access information was submitted to verify that the I-S collects only the individual's DOD ID number. The platform	e initiato	r possesses the requisite clearance level for access to AEN-S.	
f. Do	individuals have the opportunity to consent to the specific uses of	their PII?	Yes X No	
(1)	If "Yes," describe the method by which individuals can give or withhold th	eir conse	nt.	
(2)	If "No," state the reason why individuals cannot give or withhold their con	sent.		
reque colle	est system access. While applications and services found on the ct or maintain user PII other than the DoD ID number of the ind	AEN-S 1 ividuals	who access it.	
	hen an individual is asked to provide PII, a Privacy Act Statement (P ovide the actual wording.)	AS) and	or a Privacy Advisory must be provided. (Check as appropriate and	
	Privacy Act Statement Privacy Advisory	X	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.				
	ith whom will the PII be shared through data/system exchange, both heck all that apply)	within y	our DoD Component and outside your Component?	
×	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)				
X	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				

ŧ

collect or maintain Pll	
j. How will the information be collected? (Check all that apply and list all Of	fficial Form Numbers if applicable)
E-mail	Official Form (Enter Form Number(s) in the box below)
X In-Person Contact	Paper
Fax	Telephone Interview
Information Sharing - System to System	X Website/E-Form
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 th identity verification. In addition, the individual must show their Com verification before establishing their digital signature.	e DD Form 2875. The PII that is collected via the DD 2875 is used for amon Access Card to ASD personnel for purposes of identity
k. Does this DoD Information system or electronic collection require a Price of the system of the sy	rivacy Act System of Records Notice (SORN)?
A Privacy Act SORN is required if the information system or electronic collections is retrieved by name or other unique identifier. PIA and Privacy Act SORN info	on contains information about U.S. citizens or lawful permanent U.S. residents that ormation must be consistent.
If "Yes," enter SORN System Identifier	
SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Con Privacy/SORNs/ or	nponent Privacy Office for additional information or http://dpcld.defense.gov/
If a SORN has not yet been published in the Federal Register, enter date of so Division (DPCLTD). Consult the DoD Component Privacy Office for this date	
If "No," explain why the SORN is not required in accordance with DoD Regula	ation 5400.11-R: Department of Defense Privacy Program.
Although the DD 2875 is used to verify and validate users who reque Electronic Data Interchange Personnel Identifier (EDIPI), also known	est access to the AEN-S. The AEN-S only collects the individual's n as the DoD identification (ID) number, for access and audit purposes.
I. What is the National Archives and Records Administration (NARA) appr for the system or for the records maintained in the system?	roved, pending or general records schedule (GRS) disposition authority
(1) NARA Job Number or General Records Schedule Authority.	3 3.2, Item 31
(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 ide and potentially vulnerable. Destroy 6 years after password is altered o required for business use.	entification records associated with systems which are highly sensitive or user account is terminated, but longer retention is authorized if

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.
 If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar. 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 X 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.
(3) in Feiding, provide the date for the do and/or so day holice and the Federal Register Glation.
USAFRICOM AEN-S does not collect information directly from the public.

ł

	SECTION 2: PILRISK REVIEW	₩	
a. What PII will be collected (a data element alon	e or in combination that can uniquely identify ar	n individual)? (Check all that apply)	
Biometrics	Birth Date	Child Information	
X Citizenship	Disability Information	X DoD ID Number	
Driver's License	Education Information	Emergency Contact	
Employment Information	Financial Information	Gender/Gender Identification	
	Law Enforcement Information	Legal Status	
Mailing/Home Address	Marital Status	Medical Information	
Military Records	Mother's Middle/Maiden Name	Name(s)	
Official Duty Address Passport Information	Official Duty Telephone Phone Personal E-mail Address	Other ID Number	
Place of Birth	Personal E-mail Address X Position/Title	Photo Brotociad Haplith Information (BHIN)	
Race/Ethnicity	Rank/Grade	Protected Health Information (PHI) ¹ Religious Preference	
		Social Security Number (SSN) <i>(Full or in any</i>	
Records	Security Information	└── form)	
X Work E-mail Address	If Other, enter the information in the box	below	
though the above information is collected in c access. AEN-S access and audit records colle	order to grant access to AEN-S, AEN-S co ct and use only the DoD ID number.	ollects only information pertaining to audit and	
If the SSN is collected, complete the following ques	tions.		
IDoD Instruction 1000 30 states that all DoD nersor	and shall reduce or aliminate the use of SSNs w	wherever possible. SSNs shall not be used in spreadsheets.	
hard copy lists, electronic reports, or collected in su	rveys unless they meet one or more of the acce	vnerever possible. 'SSivs snall not be used in spreadsneets, aptable use criteria.)	
		,	
(1) Is there a current DPCLTD approved SSN J	Justification on Memo in place?		
Yes X No			
If "Yes," provide the signatory and date approv	val. If "No," explain why there is no SSN Justific	cation Memo.	
Neither he AEN-S registration process, nor the	e audit and access features collect or use S	SSNs for any purpose.	
(2) Describe the approved acceptable use in a	accordance with DoD Instruction 1000.30 "Redu	iction of Social Security Number (SSN) Use within DoD".	
The AEN-S does not collect or use SSNs for a	iny purpose.		
(3) Describe the mitigation efforts to reduce the Social Security Number (SSN) Use within	e use including visibility and printing of SSN in a DoD":	accordance with DoD Instructoin 1000.30, "Reduction of	
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 X 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 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			

	(1) Physical Controls. (Check all that apply) © Gottminion Locks (2) Controllation Locks (3) Security Guards (3) Security Guards (4) Administrative Controls. (Check all that apply) (2) Administrative Controls. (Check all that apply) (3) Backups Bacurity Chinak (4) Provide Controls. (Check all that apply) (5) Fortune The Information in the box below (7) Technical Controls. (Check all that apply) (6) Biometics (7) Technical Controls. (Check all that apply) (7) Technical Controls. (Check all that apply) (7) Technical Controls. (Check all that apply) (8) Information Detects (7) Technical Controls. (Check all that apply) (8) Information Detects (9) Technical Controls. (Check all that apply) (10) Technical Controls. (Check all that apply) (11) Technical Controls. (Check all that apply) (12) Tech	the Inform	tive when done in collaboration with the Information Owner, Information System Security Officer (ISSO) and Senior Component Offic	ial for Privacy (SCOP) or designe	es.	Security Manager, and repres	entatives from the security and privacy organizations, such as
Souther Locks Closed Circuit TV (CGTV) Continuation Locks Identification Badges Key Cards States It Other, enter the information in the box below (2) Administrative Controls. (Check all that apply) Backups Secured Off-eite Empryption of Backups Methods to Ensure Only Authorized Personnel Access to PII Periodic Security Aution Regular Monitoring of Users' Security Practices. If Ubner, ender the information in the box below PII holdings will be reviewed at a minimum annually to ensure the PII stored is still required. (a) Technical Controls. (Check all that apply) Biometrics Companies (b) Technical Controls. (Check all that apply) Biometrics Common Access Card (GAC) Encryption of Data at Rest Encryption of Data in Transt External Controls. Intrusion Detection System (DS) Vitual Privale Network (VPN) If Obter, 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 fill-disk encryption mechanisms to ensure that PII data-at-rest is protected from intentional or accetantal disclosure or loss. 2. Firewall - USAFRICOM employs firewall border control mechanisms that	Example Controls Closed Crew TV (CCTV) Combination Locks Intellification Badges States Safes Combination Locks Intellification Badges States Safes Backups Beauty Guards If Other, enter the Information in the box below (2) Administrative Controls. (Check all that apply) Backups Beauty Guards If Other, enter the Information in the box below (2) Administrative Controls. (Check all that apply) Backups Beauty Guards Beauty Beaut	c. How will the PII be secured?					
Souther Locks Closed Circuit TV (CGTV) Continuation Locks Identification Badges Key Cards States It Other, enter the information in the box below (2) Administrative Controls. (Check all that apply) Backups Secured Off-eite Empryption of Backups Methods to Ensure Only Authorized Personnel Access to PII Periodic Security Aution Regular Monitoring of Users' Security Practices. If Ubner, ender the information in the box below PII holdings will be reviewed at a minimum annually to ensure the PII stored is still required. (a) Technical Controls. (Check all that apply) Biometrics Companies (b) Technical Controls. (Check all that apply) Biometrics Common Access Card (GAC) Encryption of Data at Rest Encryption of Data in Transt External Controls. Intrusion Detection System (DS) Vitual Privale Network (VPN) If Obter, 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 fill-disk encryption mechanisms to ensure that PII data-at-rest is protected from intentional or accetantal disclosure or loss. 2. Firewall - USAFRICOM employs firewall border control mechanisms that	Image: Construction Locks Cleared Crewit TV (CGTV) Combination Locks Image: Cleared Crewit TV (CGTV) Combination Cleared Crewit TV (CGTV) Image: Cleared Crewit TV (CGTV) Combination Cleared Crewit TV (CGTV) Image: Cleared Crewit TV (CGTV) Combination Cleared Crewit TV (CGTV) Image: Cleared Crewit TV (CGTV) Combination Cleared Crewit TV (CGTV) Image: Cleared Crewit TV (CGTV) Cleared Crewit TV (CGTV) Image: Cleared Crewit TV (CGTV) Cleared Crewit TV (CGTV) Image: Cleared Crewit TV (CGTV) Cleared Crewit TV (CGTV) Ima	(1)	Physical Controls. (Check all that apply)				
Image: Combination Locks Image: Combination Locks Image: Key Cards States Image: Combination Locks Image: Combination Locks Image: Combinating Locks Image: Combinatinge:	Identification Eadings Identification Eadings Image: Security Guards Image: Security Guards Image: Security Guards (2) Administrative Controls. (Check all that apply) Image: Security Guards Image: Security Guards (2) Administrative Controls. (Check all that apply) Image: Security Guards Image: Security Guards (3) Administrative Controls. (Check all that apply) Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits Image: Security Audits					Closed Circuit TV (C	CTV)
Image: Solution of Security Guards Solution of Chart and Solution of	States States If Other, enter the information in the box below (2) Administrative Controls. (Check all that apply) Backups Secured Off-site (2) Administrative Controls. (Check all that apply) Security Guards (3) Technical Controls. (Check all that apply) (4) Reception of Backups (5) Administrative Controls. (Check all that apply) (5) Reception of Backups (6) Technical Controls. (Check all that apply) (7) Technical Controls. (Check all that apply) (8) Technical Controls. (Check all that apply) (9) Technical Controls. (Check all that apply) (10) Technical Controls. (Check all that apply) (11) T		Combination Locks		X	Identification Badges	5
(2) Administrative Controls. (Check all that apply) (2) Backups Secured Off-site (2) Methods to Ensure Only Authorized Parsonnel Access to PII (2) Methods to Ensure Only Authorized Parsonnel Access to PII (2) Periodic Security Audits (2) Regular Monitoring of Users' Security Practices (3) Technical Controls. (Check all that apply) (4) Technical Controls. (Check all that apply) (5) Terwall (5) Terwall (6) Terwall (7) Technical Controls. (Check all that apply) (6) Terwall (7) Technical Controls. (Check all that appl	(2) Administrative Controls. (Check all that apply) Backups Secured Off-site Encryption of Backups Wathods to Ensure Only Authorized Personnel Access to PII Periodic Security Author Regular Monitoring of Usars' Security Practicas. If Other, ease the information in the box below PII holdings will be reviewed at a minimum annually to ensure the PII stored is still required. (a) Technical Controls. (Check all that apply) Biometrics [b] Foreidits [c] Technical Controls. (Check all that apply) Biometrics [c] Technical Controls. (Check all that apply) [c] Biometrics [c] Technical Controls. [c] Technical Controls. [c] Technical Controls. [c] Notal The Markan Network (VPN) [c] Totton in advance Technical Controls are managed at an Enterprise level by USAFRICOM Joint. [c] Encryption of Data at Rest - USAFRICOM employs furvall border control mechanisms thar restrict access to PII data store dimernally on the AEN-S. [c]	X	Key Cards		X	Safes	
Image: Secure of Off-site Image: Secure of Off-site Image: Secure of Secure of Security Practices Image: Secure of Security Audits Regular Monitoring of Users' Security Practices If Other, enter the information in the box below Principal Security Audits (3) Technical Controls. (Check all that apply) Image: Security Audits (3) Technical Controls. (Check all that apply) Image: Security Audits	Seckups 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 PUI holdings will be reviewed at a minimum annually to ensure the PII stored is still required. (a) Technical Controls. (Check all that apply) Biometrics Common Access Card (CAC) Kengular Viewall Exception of Data in Transit Exception of Data at Rest Ecception of Data in Transit Kengular Viewall Enception of Data at Rest Role-Based Access Controls User Only for Privileged (Elevated Roles) Withtal Private Network (VPN) If Other, entert the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM JG: Least Privilege Access 2. Frewall - USAFRICOM employs full-disk encryption mechanisms to ensure that PII data-at-rest is protected from intentional or accidental disclosure or Iosa. 2. Frewall - USAFRICOM employs full-disk encryption mechanisms to ensure stored internally on the AEN-S. 1. Frewall - USAFRICOM employs full-disk encryption manage user access to II data stored internally on the AEN-S. 2. Frewall - USAFRICOM employs full-disk encryption mechanisms to ensure that PII data-at-rest is protected from	×	Security Guards			If Other, enter the int	formation in the box below
Image: Secure of Off-site Image: Secure of Off-site Image: Secure of Off-site Image: Secure of Security Audits Regular Monitoring of Users' Security Practices If Other, enter the information in the box below Princip Controls. (Check all that apply) Image: Security Audits (3) Technical Controls. (Check all that apply) Image: Security Audits Image: Security Audits Image: Security Audits Security Audits Security Audits Image: Security Audits <td>X Backups Secured Off-alte X Encryption of Backups X Methods to Ensure Only Authorized Personnel Access to PII X Periodic Security Audits X Regular Monitoring of User's Security Practices. X 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. (a) Technical Controls. (Check all that apply) Biometrics Cemmon Access Card (CAC) X Encryption of Data at Rest X 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 managed PI to the outified world. 2. Firewall USAFRICOM managed PI to the outified world. 3. Role-Based Access Controls - The AEN-S utilizes the DOD SIPR Token system to manage user access to II data stored internally on the AEN-S. Firewall - USAFR</td> <td>-</td> <td></td> <td>······································</td> <td></td> <td></td> <td></td>	X Backups Secured Off-alte X Encryption of Backups X Methods to Ensure Only Authorized Personnel Access to PII X Periodic Security Audits X Regular Monitoring of User's Security Practices. X 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. (a) Technical Controls. (Check all that apply) Biometrics Cemmon Access Card (CAC) X Encryption of Data at Rest X 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 managed PI to the outified world. 2. Firewall USAFRICOM managed PI to the outified world. 3. Role-Based Access Controls - The AEN-S utilizes the DOD SIPR Token system to manage user access to II data stored internally on the AEN-S. Firewall - USAFR	-		······································			
Image: Secure of Off-site Image: Secure of Off-site Image: Secure of Secure of Security Practices Image: Secure of Security Audits Regular Monitoring of Users' Security Practices. If Other, enter the information in the box below Pill holdings will be reviewed at a minimum annually to ensure the PII stored is still required. (3) Technical Controls. (Check all that apply) Image: Security Security Practices Image: Security Security Security Security Practices Image: Security Security Security Security Practices Image: Security Secu	Seckups 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 PUI holdings will be reviewed at a minimum annually to ensure the PII stored is still required. (a) Technical Controls. (Check all that apply) Biometrics Common Access Card (CAC) Kengular Viewall Exception of Data in Transit Exception of Data at Rest Ecception of Data in Transit Kengular Viewall Enception of Data at Rest Role-Based Access Controls User Only for Privileged (Elevated Roles) Withtal Private Network (VPN) If Other, entert the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM JG: Least Privilege Access 2. Frewall - USAFRICOM employs full-disk encryption mechanisms to ensure that PII data-at-rest is protected from intentional or accidental disclosure or Iosa. 2. Frewall - USAFRICOM employs full-disk encryption mechanisms to ensure stored internally on the AEN-S. 1. Frewall - USAFRICOM employs full-disk encryption manage user access to II data stored internally on the AEN-S. 2. Frewall - USAFRICOM employs full-disk encryption mechanisms to ensure that PII data-at-rest is protected from						
Image: Second Provides and Provided Personnel Access to PII Periodic Second Audits Image: Periodic Second Putting Image: Periodic Second Putting <td>Image: Second Second</td> <td>(2)</td> <td>Administrative Controls. (Check all that apply)</td> <td></td> <td></td> <td></td> <td></td>	Image: Second	(2)	Administrative Controls. (Check all that apply)				
Encryption of Backups Encryption of Backups Fegular 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. (a) Technical Controls. (Check all that apply) Biometrics Biometrics Common Access Card (CAC) Biometrics Common Access Card (CAC) DoD Public Key Infrastructure Certificates Firewall Common Access Card (CAC) External Certificate Authority Certificates Kiewall Intrusion Detection System (IDS) User Identification and Password Wirewall Private Network (VPN) If I of Data at Rest Since Controls of Data at Rest - USAFRICOM employs full-disk encryption mechanisms to ensure that PII data-at-rest is protected from intentional or accelerate al Giclosure or Ioss. 2. Firewall - USAFRICOM employs full-disk encryption mechanisms to access to PII data stored internally on the AEN-S. Firewall rules prevent exposure of USAFRICOM annaged PII to the outside world. 3. Role-Based Access Controls - The AEN-S utilizes Microsoft Active Directory to manage user access to III data stored internally on the AEN-S. Firewall rules prevent exposure of USAFRICOM managed PII to the outside world. 3. Role-Based Access to III data where the information owner grants access to III data stored internal on the AEN-S. Firewall rules prevent exposure of USAFRICOM annaged PII to the outside world. 3. Role-Based Access to III data where the information owner grants access to III data stored internal petwork resources. User Identification Transit - Through the use of the DOD SIPR Token, each user is enabled to encrypt email through DOD SIPR Token system to manage user access to USAFRICOM IT assets. Token issuance is contingent purposition structure is guarded by IDS systems that enable Cybersecurity professionals the ability to find and access net	Image: Encryption of Backups Image: Security Audits Regular Moniforing of User's Security Practices. If Other, enter the information in the box below PTI holdings will be reviewed at a minimum annually to ensure the PTI stored is still required. (a) Technical Controls. (Check all that apply) Biometrics (b) Technical Controls. (Check all that apply) Biometrics (c) Technical Controls. (Check all that apply) Biometrics (c) Technical Controls. (Check all that apply) Biometrics Common Access Card (GAC) External Certificates the information the box below (c) Technical Controls. (Check all that apply) Biometrics Common Access Card (GAC) External Certificates and the information of Data at Rest Controls Common Access Card (GAC) Yirdual Private Network (VPN) If Other, enter the information in the box betw The following technical controls are managed at an Enterprise level by USAFRICOM field 1. Encryption of Data at Rest USAFRICOM employs fill-disk encryption mechanisms to ensure that PII data-at-rest is protected from intentional or accidental disclostere or loss. 2. Firewall rules prevent exposure of USAFRICOM managed PII to the outside word. 3	×	Backups Secured Off-site				
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) Biometrics Common Access Card (CAC) X Encryption of Data at Rest X Frewall Network (VPN) Intrusion Detection System (IDS) X Least Privilege Access X Industry Private Network (VPN) X 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 firewall border control mechanisms that restrict access to PII data stored internally on the AEN-S. Firewall - USAFRICOM employs firewall border control mechanisms that restrict access to intermal network resources. 2. Firewall - USAFRICOM employs firewall border control mechanisms	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) Biometrics Common Access Card (CAC) K Encryption of Data at Rest K Intrusion Detection System (IDS) K Least Privilege Access K Note-Based Access Controls K User Identification and Password K If Other, enter the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM I6: Least Privilege Access 1. Encryption of Data at Rest - USAFRICOM employs full-disk encryption mechanisms to ensure that PII data-at-rest is protected from intentional on acceleratal disclosure or loss. 2. Firewall rules prevent exposure of USAFRICOM managed PII to the outide world. 3. Role-Based Access Controls - The AEN-S utilizes Microsoft Active Directory to manage user access to III data stored internal network resources. 4. SIPR Token- The AEN-S utilizes th DOD SIPR Token system to manage user acce	X	Encryption of Backups				
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) Biometrics Common Access Card (CAC) X Encryption of Data at Rest X Frewall Network (VPN) Intrusion Detection System (IDS) X Least Privilege Access X Industry Private Network (VPN) X 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 firewall border control mechanisms that restrict access to PII data stored internally on the AEN-S. Firewall - USAFRICOM employs firewall border control mechanisms that restrict access to intermal network resources. 2. Firewall - USAFRICOM employs firewall border control mechanisms	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) Biometrics Common Access Card (CAC) K Encryption of Data at Rest K Intrusion Detection System (IDS) K Least Privilege Access K Note-Based Access Controls K User Identification and Password K If Other, enter the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM I6: Least Privilege Access 1. Encryption of Data at Rest - USAFRICOM employs full-disk encryption mechanisms to ensure that PII data-at-rest is protected from intentional on acceleratal disclosure or loss. 2. Firewall rules prevent exposure of USAFRICOM managed PII to the outide world. 3. Role-Based Access Controls - The AEN-S utilizes Microsoft Active Directory to manage user access to III data stored internal network resources. 4. SIPR Token- The AEN-S utilizes th DOD SIPR Token system to manage user acce	X		Access to PII			
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 ell that apply) Biometrics Common Access Card (CAC) X Encryption of Data at Rest X Intrusion Detection System (IDS) X Least Privilege Access X Virtual Private Network (VPN) X If Other, enter the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM J6: Least Privilege Access 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 rules prevent exposure of USAFRICOM managed PII to the outside world. 3. Role-Based Access Controls - The AEN-S utilizes the DOD SIPR Token system to manage user access to INAFRICOM 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, systems that enable Cybersecurity professionals the ability to find and stop intrusions into the network. 6. Intrusion Detection Systems (IDS) - USAFRICOM AEN-S is	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) Biometrics Biometrics X Encryption of Data at Reat X The double at Reat X Valuel Private Network (VPN) X 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. 3. Role-Based Access Controls The AEN-S. Utilizes throwork (VPN) 4. SIPR Token- The AEN-S utilizes throwork at where the information owner grants access on the basis of need-to-know. 4. SIPR Token- The AEN-S utilizes throwork torso of Active Based Access Controls Tasets. Token issuance is contignatin type based access to PII d	X	-				
PII holdings will be reviewed at a minimum annually to ensure the PII stored is still required. (3) Technical Controls. (Check all that apply) Biometrics Common Access Card (CAC) X DoD Public Key Infrastructure Certificates X Encryption of Data at Rest Encryption of Data in Transit X Firewall Intrusion Detection System (IDS) Least Privilege Access X Role-Based Access Controls Used Only for Privileged (Elevated Roles) User Identification and Password X Virtual Private Network (VPN) If Other, enter the information in the box below User Identification and Password The following technical controls are managed at an Enterprise level by USAFRICOM JG: 1. Encryption of Data at Rest USFRICOM 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 frewall border control mechanisms that restrict access to PII data stored internally on the AEN-S. Firewall rules prevent exposure of USAFRICOM annaged 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. 4. SIPR Token- The AEN-S utilizes the DOD SIPR Token system to manage user access to use the basis of need-to-know. 4. SIPR Token- The AEN-S utilizes the DOD SIPR Token seach user is enabled to encrypt email throu	PII holdings will be reviewed at a minimum annually to ensure the PII stored is still required. (a) Technical Controls. (Check all that apply) Biometrics Common Access Card (CAC) Encryption of Data at Rest Encryption of Data in Transit External Cartificate Authority Certificates Role-Based Access Controls User Induction (DB) Witrual Private Network (VPN) If Other, enter the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM I6: I. 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 full-disk encryption mechanisms to ensure that PII data at rest resources. 3. Role-Based Access Controls - The AEN-S utilizes Microsoft Active Directory to manage user access to II data stored internally on the AEN-S. Firewall - USAFRICOM anaged PII to the outside world. 3. Role-Based Access Controls - The AEN-S utilizes the DOD SIPR Token, each user is enabled to encrypt email through DOD SIPR Token system to manage user access to USAFRICOM IT assets. Token issuance is contingent upon background vetting and user job role. 3. Encryption of Data in Transit - Through the use of the DOD SIPR Token, each user is enabled to encrypt email through DOD SIPR Token system to manage user access to USAFRICOM IT assets. Token issuance is contingent upon background vetting and user job role. 5. Encr						
(3) Technical Controls. (Check ell that epply) □ Biometrics □ Common Access Card (CAC) □ DeD Public Key Infrastructure Certificates ▼ Encryption of Data at Rest ▼ Encryption of Data in Transit □ External Certificate Authority Certificates ▼ Firewall ▼ Intrusion Detection System (IDS) ▼ Least Privilege Access ▼ Role-Based Access Controls □ Used Only for Privileged (Elevated Roles) ▼ User Identification and Password ▼ If the Network (VPN) ▼ If Other, enter the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM User Identification and Password 2. Firewall - 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 for wall border control mechanisms that restrict access to PII data stored internally on the AEN-S. Firewall - USAFRICOM employs full-disk encryption on owner grants 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 backgrou	(a) Technical Controls. (Check all that apply) Biometrics Common Access Card (CAC) DoD Public Key Infrastructure Certificates Forcyption of Data at Rest Encryption of Data in Transit External Certificate Authority Certificates K Forcyption of Data at Rest Encryption of Data in Transit External Certificate Authority Certificates K Forcyption of Data at Rest Encryption of Data in Transit External Certificate K Thread Network (VPN) K If Other, enter the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM J6: I. 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. J. 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. S. Role-Based Access Controls - The AEN-S utilizes the DOD SIPR Token system to manage user access to USAFRICOM IT assets. Token issuance is contingent user job role. S. 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 s						
Biometrics Common Access Card (CAC) X DoD Public Key Infrastructure Certificates K Encryption of Data at Rest Encryption of Data in Transit External Cartificate Authority Certificates K Firewall Intrusion Detection System (IDS) X Least Privilege Access K Role-Based Access Controls Used Only for Privileged (Elevated Roles) X User Identification and Password K Virtual Private Network (VPN) X If Other, enter the information in the box below X User Identification and Password The following technical controls are managed at an Enterprise level by USAFRICOM J6: I. 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 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 Syste	Biometrics Common Access Card (CAC) X DoD Public Key Infrastructure Certificates K Encryption of Data at Rest X Encryption of Data in Transit External Cartificate Authority Cartificates X Firewall X Intrusion Detection System (IDS) X Least Privilege Access X Virtual Private Network (VPN) X If Other, enter the information in the box below X User Identification and Password The following technical controls are managed at an Enterprise level by USAFRICOM J6: I. 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 response 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 contingen upon background vetting and user job role. 5. Intrusion Detection Systems (IDS) - USAFRICOM AEN-S is guarded by IDS systems that enable Cybersecurity professionals the ability to find and stop intrusions into t	PII ho	ldings will be reviewed at a minimum annu	ally to ensure the PII s	tored i	s still required.	
Biometrics Common Access Card (CAC) X DoD Public Key Infrastructure Certificates K Encryption of Data at Rest Encryption of Data in Transit External Cartificate Authority Certificates K Firewall Intrusion Detection System (IDS) X Least Privilege Access K Role-Based Access Controls Used Only for Privileged (Elevated Roles) X User Identification and Password K Virtual Private Network (VPN) X If Other, enter the information in the box below X User Identification and Password The following technical controls are managed at an Enterprise level by USAFRICOM J6: I. 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 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 Syste	Biometrics Common Access Card (CAC) X DoD Public Key Infrastructure Certificates K Encryption of Data at Rest X Encryption of Data in Transit External Cartificate Authority Cartificates X Firewall X Intrusion Detection System (IDS) X Least Privilege Access X Virtual Private Network (VPN) X If Other, enter the information in the box below X User Identification and Password The following technical controls are managed at an Enterprise level by USAFRICOM J6: I. 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 response 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 contingen upon background vetting and user job role. 5. Intrusion Detection Systems (IDS) - USAFRICOM AEN-S is guarded by IDS systems that enable Cybersecurity professionals the ability to find and stop intrusions into t						
Image: Second	Image: Second	(3)	Technical Controls. (Check all that apply)	· ····			
Image: Strewall Intrusion Detection System (IDS) Image: Least Privilege Access Image: Strewall Role-Based Access Controls Used Only for Privileged (Elevated Roles) Image: User Identification and Password Image: Strewall Role-Based Access Controls Used Only for Privileged (Elevated Roles) Image: User Identification and Password Image: Strewall Role-Based Access Controls If Other, enter the information in the box below Image: User Identification and Password The following technical controls are managed at an Enterprise level by USAFRICOM J6: I. 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 aules 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 resources to network resources c	Image: Strewall Intrusion Detection System (IDS) Image: Strewall Access Controls Image: Strewall Private Network (VPN) Image: Strewall Access Controls Image: Strewall Access Controls Image: Strewall Private Network (VPN) Image: Strewall Access Controls Image: Strewall Access Controls Image: Strewall Private Network (VPN) Image: Strewall Access Controls Image: Strewall Access Controls Image: Strewall Private Network (VPN) Image: Strewall Access Controls Image: Strewall Access Controls Image: Strewall Private Network (VPN) Image: Strewall Access Controls Image: Strewall Access Controls Image: Strewall Private Network (VPN) Image: Strewall Access Controls Image: Strewall Access Controls Image: Strewall Private Network (VPN) Image: Strewall Access Controls Image: Strewall Access Controls Image: Strewall Private Network (VPN) Image: Strewall Control Methods Image: Strewall Control Methods Image: Strewall Private Network Strewall Private Network Image: Strewall Private Network Image: Strewall Private Network Image: Strewall Private Network Private Network Private Network Image: Strewall Private Network Image: Strewall Private Network Image: Strewall Private Network Image: Strewall Privat		Biometrics	Common Access C	ard (C	AC)	X DoD Public Key Infrastructure Certificates
Virtual Private Network (VPN) 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 reso	 Virtual Private Network (VPN) If Other, enter the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM J6: 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. Firewall - USAFRICOM employs firewall boder control mechanisms that restrict access to PII data stored internally on the AEN-S. Firewall - USAFRICOM managed PII to the outside world. 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 graatest 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. HBS	×	Encryption of Data at Rest			•	
Virtual Private Network (VPN) 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 reso	 Virtual Private Network (VPN) If Other, enter the information in the box below The following technical controls are managed at an Enterprise level by USAFRICOM J6: 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. Firewall - USAFRICOM employs firewall border control mechanisms that restrict access to PII data stored internally on the AEN-S. Firewall - USAFRICOM managed PII to the outside world. 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. HB	X		Laurand Control of Con			
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 -	 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 TASK				- :		X User Identification and Password
 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. 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. 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. 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. 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. 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. 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. 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 Websites - HBSS - 	 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. 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. 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. 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. 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. 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. 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. 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 Wherability 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 Asses					·····	·····
 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 - 	 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 USAFRCIOM Informat						that DIL data at most is much at all forms
 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 - 	 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 USAFRICIOM Information Systems. The tool i		• • •	bloys full-disk encrypt	ion m	echanisms to ensure	e that PII data-at-rest is protected from
 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 - 	 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 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 pu	í		ler control mechanism	s that	restrict access to PII	data stored internally on the AEN-S.
 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 - 	 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 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? 						
 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 - 	 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 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 are responsible for maintaining data integrity and 						
 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 - 	 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 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? 						
 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 - 	 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 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? 				inage	user access to USAI	FRICOM 11 assets. Token issuance is
 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 - 	 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 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? 				ken, e	ach user is enabled	to encrypt email through DOD SIPR
 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 - 	 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 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? 	1			, .		
 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. 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 Websites - HBSS - 	 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 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? 			OM AEN-S is guarde	d by II	DS systems that ena	ble Cybersecurity professionals the ability
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 -	 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 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 are responsible for maintaining data integrity and 						
 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 - 	 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 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 are responsible for maintaining data integrity and 						
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 -	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 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 are responsible for maintaining data integrity and						
passwords are enforced through Enterprise Active Directory control mechanisms. Secret Internet Protocol Router Network (SIPRNet) Token 10. Websites - 11. HBSS -	 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 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? 						
10. Websites - 11. HBSS -	 10. Websites - HBSS - HBSS -						
11. HBSS -	 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 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 are responsible for maintaining data integrity and 	ł					
	 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 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 are responsible for maintaining data integrity and 						
12.7 and $a0107$ management in accordance with OCCI DERCOM TROPORT 110012, I RACE TO TROPORT 10 TROPORT 110012,	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 are responsible for maintaining data integrity and						
	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 are responsible for maintaining data integrity and						
mandated Vulnerability Scanning tool for USAFRCIOM Information Systems. The tool is utilized for required Weekly Vulnerability	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						
Scanning, STIG Configuration, and Network Vulnerability Monitoring.	Complete access to all records is restricted to and controlled by the data owner who are responsible for maintaining data integrity and	Scann	ing, STIG Configuration, and Network Vul	nerability Monitoring.			
Complete access to all records is restricted to and controlled by the data owner who are responsible for maintaining data integrity and confidentiality.	confidentianty.			controlled by the data	owne	r who are responsib	le for maintaining data integrity and

ł