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:

U.S. Africa Command (USAFRICOM) United States Battlefield Information Collection and Exploitation Systems Extended (USBICES-X) Commercial Solutions for Classified Network (CSfC)

2. DOD COMPONENT NAME:

United States Africa Command

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

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

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

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

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

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Directorate of Capabilities uses a series of Capability Packages (CPs) to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The USAFRICOM USBICES-X CSfC network follows the NSA-provided high-level reference designs and corresponding configuration information that allow customers to select COTS products from the CSfC Components List, available on the CSfC web page (https://www.nsa.gov/resources/everyone/csfc), for their solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. Customers ensure that the components selected from the CSfC Components List will permit the necessary functionality for the selected capabilities.

US BICES-X is a Coalition sharing network between partner nations and the United States Military. US BICES-X allows U.S. users to access partner nation secure networks and is the mechanism by which all U.S. producers disseminate releasable intelligence products and data into the BICES-X environment. The USAFRICOM AC networks are coalition networks that specifically supports the USAFRICOM intelligence mission. The AC Networks use the USAFRICOM USBICES-X CSfC network for network transport. The USBICES-X, AC Networks, and USAFRICOM USBICES-X CSfC network are supported by third party contractor, General Dynamics Information Technology (GDIT).

To gain access to the USAFRICOM USBICES-X CSfC network, users must request an account by completing and submitting a DD 2875 form to their supervisor for verification. The Form DD 2875 requires users to provide their full name, official email address, official work address, DoD ID and supervisor name. Once verified by their supervisor and the Terminal Area Security Officer (TASO), the completed DD 2875 is submitted via email to the Coalition Service System Desk (CSSD) for identification and verification of eligibility. The CSSD then uploads the DD 2785 to US BICES-X portal for tracking purposes. If the individual is a US citizen, the CSSD sends an email to the individual's Security Officer (SO).

US citizens who request access to the system may be contacted by their SO to provide their Social Security Number (SSN) if their DoD ID is unavailable or the system cannot verify clearance by the DoD ID alone. The SSN may be provided in person, if the individual is co-located with their SO, if the SO is not on site, an email will be sent to the individual to call the SO. The individual will then call the SO to provide her or him with their SSN. If the US citizen is unwilling to provide their SSN, they may provide their Date of Birth (DOB) as an alternative. Once the SO has acquired the individual's SSN or DOB, they will use DMDC Joint Personnel Adjudication System (JPAS) or the Defense Information Security System (DISS) to verify that the individual has the appropriate clearance for the level of access that they are requesting. The clearance level of the individual requesting access is then input on the DD 2875 and the SO places their digital signature on the

document. Neither the SSN nor DOB are notated anywhere on the DD 2875. The SO sends the DD 2875 to the CSSD via US BICES-X, NIPRNet, or SIPRNet. Once the DD 2875 is collected, it is disseminated via email on NIPRNet or SIPRNet. DD 2875s are not stored on the USAFRICOM USBICES-X CSfC network. DD 2875s are only stored in separate files on SIPRNet or on US BICES-X main system.

The USAFRICOM USBICES-X CSfC network uses the DD 2875 to create the user account and the user is sent an encrypted email. The email contains a temporary password that the user will use to authenticate to the system. When logging in for the first time, the user will enter their username (firstname.lastname.role) and temporary password to access the system. The temporary password must be changed after a successful first login. The user will use that username and new password until prompted to change the password in accordance with security policy. All users authenticate to this system using the same method. Authenticated users are authorized permissions based on their role in accordance with the CSfC Role-based Access Control (RBAC) Matrix.

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

Identification: In order to access the system, users must request an account using the Form DD 2875. The DD 2875 requests that users provide their full name, official email address, official work address, and supervisor name. Once the individual has been identified. This information is used to verify eligibility for system access and to authenticate the individual for system access. The DD 2875 is used to verify eligibility to access the network. Once the requesting user is verified for eligibility, a general user account is created by the US BICES-X Coalition System Service Desk, the user is then provided their user name (firstname.lastname.role) and a temp password to use to create their own password.

e. Do individuals have the opportunity to object to the collection of their PII? [X] Yes [ ] No

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

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

Individuals can object to the collection of their PII collected by the DD 2875 by not submitting it. However, no account would be created and the individual would not get access. Individuals are informed of this via a Privacy Act Statement that is found on the DD 2875. The SSN may be requested from US citizens in order to verify that they possess the proper security clearance for the level of access requested if the verifying system is unable to do so by DoD ID alone. If the individual does not wish to provide their SSN, they may provide their Date of Birth. However without one of these identifiers, access could not be granted to the US citizen users.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] Yes [ ] No

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

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

Individuals are not specifically provided with the opportunity to consent to the way in which their information is used; however, users are aware that the PII that they submit via the DD 2875 will be used to verify eligibility of an individual to create a user or privileged user account that will enable them authenticate system access. Without the information provided via the DD 2875 (and for US citizens, verification by the SO that the individual has the proper level of clearance) it is not possible to create an account for the requester.

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

[X] Privacy Act Statement [ ] Privacy Advisory [X] Not Applicable

The Privacy Act Statement found on the DD Form 2875 states:

Authorities: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

Purpose: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Uses: None.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

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

[X] Within the DoD Component	Specify.	Supervisor/Terminal Area Security Officer/Information System Owner/Information System Security Manager
[ ] Other DoD Components	Specify.	
[ ] Other Federal Agencies	Specify.	
[ ] State and Local Agencies	Specify.	
[ ] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
[X] Other *(e.g., commercial providers, colleges).*	Specify.	GDIT

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

- [ ] Individuals
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [X] Databases
- [ ] Commercial Systems

US BICES-X or shared files on SIPRNet.

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

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

Once the DD 2875 is collected, it is disseminated via email on NIPRNet, SIPRNet, or US BICES-X. DD 2875 are not stored on the USAFRICOM USBICES-X CSfC network. DD 2875s are only stored in separate, shared files on SIPRNet or on the US BICES-X main system.

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

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

[ ] Yes [X] No

If "Yes," enter SORN System Identifier

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

or

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

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

The USAFRICOM USBICES-X CSfC network does not retrieve information about users using a personal identifier.

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

(1) NARA Job Number or General Records Schedule Authority. GRS 3.2, Item 30-31, System access records; CJCSM Series 0300-01,

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

(3) Retention Instructions.

GRS 3.2 System Access Records
Item 30: Systems not requiring special accountability for access: Destroy when temporary business uses ceases.
Item 31: Systems requiring special accountability for access: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized for business use.

CJCSM 5760.01A, Vol. II
0300-01, Short-Term records related to intelligence and security are records that have minimal or no documentary or evidential value. - Destroy/Delete after 180 days.
0300-03, Intelligence General Correspondence Files - Destroy/Delete no less than 7 years and no more than 10 years after cutoff.
0300-04Intelligence Projection Records - Transfer legal custody of electronic records to the National Archives 25 years after cutoff, after declassification review.

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

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

10 U.S.C. 137, Under Secretary of Defense for Intelligence; Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act; Executive Order (E.O.) 10450, and E.O. 9397, as amended. The DoD ID, SSN or DOB is only used when identifying/locating an individual in JPAS or DISS.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ Yes ☒ No ☐ Pending

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

The information collected via the DD 2875 process is used to provide users with access to an internal DoD information system. Information is not requested from the public. USAFRICOM USBICES-X CSfC does not access the information provided on the DD 2875.

SECTION 2: PII RISK REVIEW

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

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

While the DoDID is collected and SSN/DOB may be collected from US citizens in order to determine appropriate level of access to the system, the USAFRICOM USBICES-X CSfC network do not store the DoDID, SSN, DOB or any other PII. Once registered, system access is provided via the username (firstname.lastname.role) and a password.

If the SSN is collected, complete the following questions.

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

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☒ No

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

While the SSN is requested is for verification of appropriate level of access in JPAS or DISS. This verification is done completely outside of the system. The SSN (or PII other than name) is never entered into or used by USAFRICOM USBICES-X CSfC for any purpose.

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

N/A

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

Only personnel with a required "need to know" have access to the view records stored as a repository and are limited by role-based permissions.

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

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

☐ Yes ☒ No

The PII that is collected via the DD 2875 process is used to provide users with access to an internal DoD information system. USAFRICOM USBICES-X CSfC does not access the information provided via the DD 2875 process.

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

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

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

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

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

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

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

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

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

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

PII used to determine eligibility for system access is collected and disseminated by US personnel who have an appropriate background check and a need-to-know to process the DD 2875 (SOs/Program Managers/Program Supervisors/CSSD personnel). When used, the DoDID/SSN/DOB is only accessed by properly cleared SO with a need to know in order to verify the appropriate clearance for the requested level of access level. PII is never not entered into or used by the USAFRICOM USBICES-X CSfC network.