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:

Software-Defined Data Center Out-of-Band Management (SDDC OBM)

2. DOD COMPONENT NAME:

United States Africa Command

3. PIA APPROVAL DATE:

09/21/21

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 SDDC OBM is US BICES-X management platform for M-DRIVE, the cross-domain solution for the Software-Defined Data Center (SDDC). The M-DRIVE system addresses technical limitations in the SDDC enclave coalition network operations to deliver a more effective solution for coalition communications by providing the ability to host and scale multiple Secret Releasable networks; to mitigate loss of communication through physical infrastructure swaps (i.e., replacing end-of-service rack-mounted servers in data centers). The SDDC solution provides secure data access to multiple Bilateral networks (BILATS) within the U.S. Africa Command Enterprise Network.

US BICES-X is a Bilateral sharing network between partner nations and the United States military. BICES-X consists of software, hardware and integrated processes designed to help U.S. and foreign allies collaborate at the national and tactical levels through intelligence data exchange. The system consists of basic file sharing, voice, email, chat capabilities, to include a separate Cross Domain Solution (CDS) to allow the exchange of information across differing security domains. US BICES-X is deployed in hundreds of locations around the world. Non-U.S. users access the central US BICES-X backbone from locations within partner nations. 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 BILATS portion of US BICES-X consists of coalition networks that specifically supports the USAFRICOM intelligence mission. The system is supported by third party contractor, General Dynamics Information Technology (GDIT).

To gain access to the SDDC OBM, users must request an account by completing and submitting a DD 2875 to their supervisor for verification. The Form 2875 requires users to provide their full name, official email address, official work address, DoDID and supervisor name. Once verified by their supervisor and the Security Officer (SO), 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 SO.

US citizens who request access to the system may be contacted by their SO to provide their Social Security Number (SSN) if their DoDID is unavailable or the system cannot verify clearance by the DoDID 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 DD2875 to the CSSD via US BICES-X. Once the DD 2875 is collected by the CSSD, it is disseminated via email on Non-classified Internet Protocol Router Network (NIPRNet) or Secret Internet Protocol Router Network (SIPRNet). DD 2875s are not stored on NIPR, the AC BILAT enclaves or its management

components. DD 2875s are only stored in separate files on SIPRNet or on US BICES-X main system but not SDDC OBM.

SDDC OBM administrators use 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 Role-based Access Control (RBAC) Matrix, a spreadsheet that defines permissions granularly based on user roles.

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: 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, DoDID and supervisor name. This information is used to verify eligibility by checking credentials to authenticate the individual for SDDC OBM system access. The outcome of this validation is than relayed to the ISSM. The ISSM sends an email to the SDDC OBM System Administrators (SA) requesting the user account/role setup. Once created, the SA provides the user name (firstname.lastname.role) and a temporary password. He or she must change immediately after a successful logon. US BICES-X archives the DD 2875.

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 by the SDDC OBM and the individual would not receive 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 for the Security Officer to verify, via JPAS or DISS that the individual possesses the proper security clearance for the level of access requested. If the individual does not wish to provide their SSN, they may provide their Date of Birth. However without one of these identifiers, access to SDDC OBM cannot be granted to 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 the information that they submit via the DD 2875 will be used to verify eligibility of an individual in order to create a user or privileged user account, which will enable the individual to authenticate to the system for 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) the SDDC OBM is unable 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 for
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 who does not provide PII to the SDDC OBM

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 by the CSSD, it is disseminated via email on Non-classified Internet Protocol Router Network (NIPRNet) or Secret Internet Protocol Router Network (SIPRNet), and on US BICES-X. DD 2875 are not stored on NIPR nor the AC BILAT management systems, components or enclaves. DD 2875s are stored in separate files on SIPRNet (not within the AC BILAT management systems, components or enclaves) or on US BICES-X main system . The US BICES-X system is separate from the AC BILAT management systems, components and enclaves, on which SDDC OBM is located.

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.

DOD US BICES-X AC BILAT, the underlying system for SDDC OBM management systems, components and enclaves do 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.
0300-04, Intelligence 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.

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.

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 DoD ID and SSN/DOB may be collected from US citizens in order to determine appropriate level of access to the system pursuant to the 2875 process, the SDDC OBM does not store the DoD ID, SSN, DOB or any PII aside from name. Once registered, access is via 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.

The only time a DoD ID is requested is to allow the SO to verify appropriate security clearances using JPAS or DISS access verification purposes. As stated above, verification is done completely outside of BICES-X AC BILAT management systems, components or enclaves. The DoD ID (or any PII other than name) is not entered into or used by the system 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".

(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

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

The 2875 to include user account request paperwork is transmitted outside of the AC BILAT enclaves via SIPR email. Staff must be cleared in order to gain access to spaces where SIPR is available. Again, at no point is any content from the DD2875 entered into or maintained by the AC BILAT enclaves.

(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 DoD ID/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 US BICES-X AC BILAT management systems, components or enclaves.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

☐	Yes, DITPR	DITPR System Identification Number	
☐	Yes, SIPRNET	SIPRNET Identification Number	
☒	Yes, RMF tool	RMF tool Identification Number	2397
☐	No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

☐	Authorization to Operate (ATO)	Date Granted:	
☐	ATO with Conditions	Date Granted:	
☐	Denial of Authorization to Operate (DATO)	Date Granted:	
☐	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

The eMASS package is currently in the Categorization phase of RMF (Step 1). The project goal is to complete Control Implementation (Step 3) and submit to the Package Approval Chain (PAC) for Control Assessment (Step 4) and ATO (Step 5) by Feb 2022.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

☐ Yes ☒ No

If "Yes," Enter UII _____ If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Haresh C. Singh	(1) Title	USAFRICOM US BICES-X ISSM
(2) Organization	USAFRICOM US BICES-X J69	(3) Work Telephone	+44 (0) 148084 2803
(4) DSN	314-268-2803	(5) E-mail address	haresh.c.singh.ctr@mail.mil
(6) Date of Review	09/02/21	(7) Signature	SINGH.HARESH.CHANDRA.1412328708 Digitally signed by SINGH.HARESH.CHANDRA.1412328708 Date: 2021.09.03 11:00:45 +01'00'
b. Other Official ***(to be used at Component discretion)***		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
c. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
d. Component Privacy Officer (CPO)	Brian F. Bullock	(1) Title	Privacy, Civil Liberties, and Transparency Officer
(2) Organization	USAFRICOM J033	(3) Work Telephone	+49 (0) 7117 0810339
(4) DSN	324.591.0339	(5) E-mail address	brian.f.bullock.civ@mail.mil
(6) Date of Review	09/10/21	(7) Signature	BULLOCK.BRIAN.FRANKLIN.1268082693 Digitally signed by BULLOCK.BRIAN.FRANKLIN.1268082693 Date: 2021.09.10 09:09:54 +02'00'

e. Component Records Officer	Daniel E. Sewell	(1) Title	Command Records Manager
(2) Organization	J033	(3) Work Telephone	324-591-0336
(4) DSN		(5) E-mail address	daniel.e.sewell.civ@mail.mil
(6) Date of Review	09/09/21	(7) Signature	SEWELL.DANIEL.E.1019720361 Digitally signed by SEWELL.DANIEL.E.1019720361 Date: 2021.09.10 07:51:16 +02'00'
f. Component Senior Information Security Officer or Designee Name	KENNETH D. STACY	(1) Title	U.S. Africa Command Chief Information Security Officer
(2) Organization	HQ USAFRICOM/J62	(3) Work Telephone	324-591-6200
(4) DSN		(5) E-mail address	kenneth.d.stacy.civ@mail.mil
(6) Date of Review:	09/21/21	(7) Signature	STACY.KENNETH.DALE.1149789266 Digitally signed by STACY.KENNETH.DALE.1149789266 Date: 2021.09.21 09:06:18 +02'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name	Brian F. Bullock	(1) Title	Privacy, Civil Liberties, and Transparency Officer
(2) Organization	US AFRICOM J033	(3) Work Telephone	+49 (0) 7117 0810339
(4) DSN	324-591-0339	(5) E-mail address	brian.f.bullock.civ@mail.mil
(6) Date of Review	09/21/21	(7) Signature	BULLOCK.BRIAN.FRANKLIN.1268082693 Digitally signed by BULLOCK.BRIAN.FRANKLIN.1268082693 Date: 2021.09.21 11:00:45 +02'00'
h. Component CIO Reviewing Official Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review	09/21/21	(7) Signature	

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.