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 public website, www.africom.mil

2. DOD COMPONENT NAME:

United States Africa Command

3. PIA APPROVAL DATE:

09/03/20

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- [X] From members of the general public
- [ ] 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 U.S. Africa Command public website, www.africom.mil, is used to inform members of the general public of United States Africa Command (AFRICOM) alliances, exercises and other activities. The website also serves as a central location for AFRICOM personnel to locate helpful resources, based upon location of his or her assignment and role. The links provided are a mix of informational resources and tools for fulfillment of official duties. The AFRICOM Public Affairs website uses persistent cookies only to "remember: visitors for the purpose of improving the user experience. These cookies are not used to track or monitor user activities when not on the AFRICOM website.

The website has a Contact Us feature that allows members of the public to submit questions or provide feedback to AFRICOM. A user who wishes to submit feedback is asked to provide a name and an email address when submitting a question or feedback. If he or she wishes to submit information anonymously, the individual may provide an alias/pseudonym as name. While a valid e-mail is required to submit the form, the email address can be an email the user creates specifically to ask a question or to submit information. Once a question is submitted, it is routed to a Public Affairs Office organizational mailbox for action. If public affairs needs information from another or other AFRICOM offices in order to respond, the contents of the email are forwarded for input. While the email address of the person/organization to whom the email was sent is recorded by the content manager, during internal routing, the name of the individual who submitted the request and the email address provided are not visible.

The website also has "Civilian Casualty Reporting" feature that allows members of the public to provide informations regarding allegations of civilian casualties that may have resulted from AFRICOM operations. This feature is intended to make the reporting of such alleged incidents as easy as possible so that assessments can be conducted and allegations can be determined as substantiated or unsubstantiated. The Contact Us, and Civilian Casualty Reporting features are the only places where information is collected directly from the public. The Civilian Casualty Reporting feature requests a phone number or e-mail, to enable AFRICOM to follow up with the submitter of the information, however, the submission of this information is not required in order to submit an allegation. Once the submitter submits the form, the system-generates and e-mail that is sent to designated users or distribution lists.

The staff of the Public Affairs Office manage website content. In order to manage content, they must log-in to the content management system using the log-in e-mail address that has been registered with Microsoft Azure The system uses 2-factor authentication. Once the individual has logged-in to the content manager, they receive a telephone call to the phone number registered to Microsoft Azure. This call is used to both notify the user that their account is being accessed, and to authenticate him or her as the user. Once the user is authenticated, she or he is automatically logged into the system.

The Sysadmins, develop, maintain and sustain the website and the back end Platform as a Service. The Sysadmins also update and manage user accounts. Azure Administrators authenticate to portal.azure.com for web application and user administration using Microsoft multi-

factor authentication (user credentials and/or verification codes sent to an assigned phone or via the MS Authenticator mobile application). Accounts are managed by CITS Software Engineering Azure admins according to the User Management Policy guide, which is available as an artifact in the ATO package.

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

The PII of external users is only used to contact the user submitting questions/comments. It is not stored or used for any other use. The system stores the e-mails for various offices on the backend and a system-generated e-mail is sent to the back-end user.

Public Affairs Office staff must submit a request of access. Once their identity is verified, they are approved for access, and are issued a log-in address that is specific to that user. That log-in address is then used to authenticate users before they are permitted into the system using these credentials. Azure SysAdmins follow a similar account creation process and are vetted/assigned necessary roles by the CITS Software Engineering Lead (global administrator).

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.

For public users, completion of the Contact Us and Civilian Casualty Reporting features are entirely voluntary. While names are requested, aliases /pseudonyms can be used. A valid e-mail is required for a response to be provided. Users may also elect to provide additional PII, but it is not requested.
Public Affairs Office staff may must provide their name, business email, and work telephone number for access to the Content Management system. Failure to provide this information will preclude them from logging in to the system. System Administrators follow an identical process for access to the Content Management System (CMS).

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.

Public users who provide personal contact information, using either the Contact Us or the Civilian Casualty Reporting feature, are assumed to want to be contacted by the command, as they voluntarily provide and submit that information. Their personal contact information is provided for very specific purposes, and used only for the purposes for which it was provided. Public Affairs Office staff and SYSADMINs provide their PII in order to gain access to the system and make changes to content or users profiles.

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

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

While the system collects PII (name, personal email, and/or personal telephone) from the public, the PII that is collected is not used for the purpose of retrieving other information about the individual to whom it pertains. Login and authentication information (login and password) is collected, but a PAS is not provided, as the information is linked to an account, and not to an individual.

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.	It is only is shared with the members of the office the user would like to respond to their report, comment, or inquiry.
[ ] 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.

☐ Other *(e.g., commercial providers, colleges).* Specify.

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

☒ Individuals
☐ Databases
☐ Existing DoD Information Systems
☐ Commercial Systems
☐ Other Federal Information Systems

The Contact Us form is an available as an optional tool for site users to contact the USAFRICOM command via e-mail for inquiries or an area of concern. The form prompts for first name, last name and e-mail address so a command representative may properly respond. This data is not stored by the system, and is sent to the component distro-address via e-mail.

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

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

The Contact Us feature of the website is used to collect contact information from members of the public. For internal users, e-mail, face-to-face contact, and telephone conversations are used to collect information needed to establish user accounts and to to access the content. management 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 ☒ 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.

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. NARA GRS 3.2, Item 030; and GRS 5.2, Item 010

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

(3) Retention Instructions.

System Access Records - NARA GRS 3.2, Item 30 - Destroy when business use ceases. The Web pages themselves are considered transitory records and are maintained in accordance with GRS 5.2, Item 010, Destroy when no longer needed for business use, or according to

predetermined time period or PAO business rules.

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. 113, Secretary of Defense; 10 U.S.C. 161, Combatant Commands: establishment; 10 U.S.C. 164, Commanders of combatant commands: assignment; powers and duties.

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	

Members of the public must provide personal email addresses to submit comments or questions via the Contact Us feature. Members of the public who wish to submit information via the Civilian Casualty Reports feature, must provide a name, and may choose to provide email address and/or personal telephone number. Public Affairs Office staff must provide Work or personal cell phone and work e-mail address for two factor authentication when logging into the website content manager. The CMS users login to the application to upload Command content for the website.

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.

(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".

(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
- [X] Key Cards
- [X] Security Guards
- [X] 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)
- [ ] Common Access Card (CAC)
- [X] Encryption of Data in Transit
- [X] Intrusion Detection System (IDS)
- [X] Used Only for Privileged (Elevated Roles)
- [ ] If Other, enter the information in the box below
- [ ] DoD Public Key Infrastructure Certificates
- [X] 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?

Two-factor authentication (login address and password, plus phone call for internal users).