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 Facebook Page

2. DOD COMPONENT NAME:

United States Africa Command

3. PIA APPROVAL DATE:

10/15/20

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
- [ ] From Federal employees and/or Federal contractors
- [x] 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
- [ ] 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.

U.S. Africa Command (AFRICOM) uses Facebook, a publicly available social networking website, to disseminate information to the public. AFRICOM currently maintains four specific Facebook pages: the main, English-language page and three foreign language pages (Arabic, French, and Portuguese) created and administered by the Public Affairs Office (PAO).

The AFRICOM Facebook pages can be accessed online at:

www.facebook.com/AFRICOM
www.facebook.com/AFRICOM.Arabic
www.facebook.com/AFRICOM.French
www.facebook.com/O-Comando-dos-EUA-para-%C3%81frica-Africom-550799138376432 (Portuguese)

These Facebook pages allow AFRICOM to provide various audiences a deeper understanding of AFRICOM, its missions and the timely release of information. The type of content posted on J035 social media platforms is intended to inform and educate audiences about the command and its missions and operations.

These pages are available to the public, and individuals do not need to register for a Facebook account to see the AFRICOM's Facebook page content. The vast majority of AFRICOM's content on Facebook is also available on the AFRICOM Website. If users wish to actively engage with AFRICOM on Facebook, they must register and are subject to Facebook's Terms of Service. Users who interact with AFRICOM on Facebook may like, comment on, and share the content created by AFRICOM. These types of interactions add a viral marketing component to the Command's outreach and education efforts.

The FTC also intends to use Facebook's "Live" feature, which allows the agency to share live videos with staff, media, partners, etc. Use of Facebook Live allows USAFRICOM to provide answers to audience questions or comments in real time and demonstrates the Command's commitment to enhanced transparency.

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)*

Individual users who register with Facebook are required to provide a first name, last name, valid email address, password, sex, and date of birth to create a personal Facebook profile. Once registered, users have the option to provide a wealth of additional information about themselves such as telephone number, interests, employment, etc., which may be displayed on the individual user's personal Facebook profile page or otherwise maintained or used by Facebook. This information, if provided in the user profile, may be available to AFRICOM in whole or part, based on a user's privacy settings.

Where authorized or required by law, AFRICOM may view, read, review, or rely on information that users of Facebook make available to the public or directly to AFRICOM. However, AFRICOM does not routinely solicit, collect or maintain PII of members of the public. Nor does it routinely disseminate the unsolicited PII. AFRICOM may collect usernames of individuals who post messages directly to AFRICOM or AFRICOM staff that are deemed threatening or potentially violent. Additionally, AFRICOM may also occasionally produce reports or summaries of its use of this social media platform that include PII that is posted publicly (i.e., usernames) as part of its Federal records retention obligations.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

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

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

All information about an individual that is available on the AFRICOM Facebook page is made available to AFRICOM because the individual liked, commented on, or shared a post. The only information that is available to AFRICOM is the username and the information that the individual chose to provide.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☐ Yes ☒ No

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

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

AFRICOM does not use the PII of an individual for any purpose other than for purposes of identifying users who post violent or threatening to AFRICOM or its staff, or to produce summaries of its use of the Facebook social media platform that may include information that is publicly posted in order to meet its Federal records retention obligations. Users who simply visit the Facebook page and either 1) do not have a Facebook account or 2) are not logged in/do not interact with the page, do not make any PII available to AFRICOM Facebook administrators.

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

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

It is important to note that the Facebook page is not the official AFRICOM website. Facebook is controlled and operated by a third party and is not a government website or application. Therefore, AFRICOM is unable to provide any assurance that the information being collected by Facebook and its application providers will adhere to the Privacy Act of 1974 or any other Federal requirement. By accessing AFRICOM's Facebook page, users may be providing non-government third parties access to their personal information, which can be used to distinguish or trace the individual's identity. Additionally, Facebook and its application providers may use persistent technology throughout their sites. Users must consent to this when they accept the Facebook Terms of Service. AFRICOM may exercise limited control over the sharing of PII on its Facebook pages by deleting individual comments, consistent with its commenting policy, if an individual posts unnecessary amounts of PII.

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

☐ Within the DoD Component	Specify.	
☐ Other DoD Components	Specify.	
☒ Other Federal Agencies	Specify.	Posts, which include username, may be shared with NARA for records management auditing purposes.
☐ 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.	There is a possibility that other third party applications may access and share user information. For example, links posted by the FTC may lead to third-party, non-government websites that may have different privacy policies than those of Facebook or AFRICOM. Facebook and its application providers may use persistent technology throughout their sites.

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

All information (username and comment content) is provided to the USAFRICOM website from users who interact with the Command on Facebook by liking, commenting on, or sharing USAFRICOM news and information.

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)*

As AFRICPOM posts updates on its Facebook pages, individuals sometimes comment on the updates. These comments may include PII from the individual making the comment, such as their user names. Users who simply visit the Facebook page and either 1) do not have a Facebook account or 2) are not logged in/do not interact with the page, do not make any PII available to AFRICOM Facebook administrators.

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.

Facebook is controlled and operated by a third party and is not a government website or application. Therefore, AFRICOM is unable to provide any assurance that the information being collected by Facebook and its application providers will adhere to the Privacy Act of 1974 or any other Federal requirement.

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 6.4, Item 020, Public Comments and Communications not

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

(3) Retention Instructions.

Comments received by AFRICOM are subject to destruction when 90 days old, but longer retention is authorized if required for business use. However, AFRICOM Facebook page administrators have limited ability to delete users and/or their comments, hide posts, and block users, as noted earlier. Staff deletes comments that violate AFRICOM's comment policy, which is outlined on each of its Facebook pages. AFRICOM does not maintain any record of deleted comments nor do they notify users that their comments have violated the comment policy.

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. Additionally, the President's January 21, 2009 memorandum on Transparency and Open Government and the OMB Director's December 8, 2009 Open Government Directive call on federal departments and agencies to harness new technologies to engage with the public. Using tools to communicate with the public and USAFRICOM partners on platforms where they are active help to meet the federal guidance outlined in the directive and memorandum including transparency, participation and collaboration.

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.

Per the OMB memorandum, Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (April 7, 2010) and DoD Manual 8910.01, Volume 2, the USAFRICOM's use of Facebook is not an information collection activity that would trigger the requirements of Act.

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	

Individual users who register with Facebook are required to provide a first name, last name, valid email address, password, sex, and date of birth to create a personal Facebook profile. Once registered, users have the option to provide a wealth of additional information about themselves such as telephone number, interests, employment, etc., which may be displayed on the individual user's personal Facebook profile page or otherwise maintained or used by Facebook. This information may or may not be available to USAFRICOM and others, in whole or part, based on a user's privacy settings.

Consumers who simply visit AFRICOM's Facebook pages and either 1) do not have a Facebook account or 2) are not logged in/do not interact with the page, do not make any PII available to AFRICOM Facebook administrators

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)*

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

In general this does not apply.

(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

AFRICOM does not routinely use Facebook to solicit, collect, maintain, or disseminate PII from members of the public. Regarding the limited instances in which the FTC does so, AFRICOM follows the methods laid out in privacy and security policies to secure all agency PII. Any copies of comments or other user interactions on Facebook maintained for law enforcement or record auditing purposes are subject to applicable Federal privacy and information security laws.

Facebook, not AFRICOM controls the security of comments or other information posted on that site. Facebook users should review Facebook's terms of service and privacy policies for information regarding the security of that site.

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

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

Facebook controls the security of comments or other information posted on that site. Facebook users should review Facebook's terms of service and privacy policies for information regarding the security of that site.

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