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 Twitter 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.)*

- [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
- [ ] 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.

Twitter is a free social networking and micro-blogging service that enables users to send and read messages called tweets. Tweets are text-based communications, or posts, of up to 280 characters, which may contain abbreviated text and URLs. Tweets are displayed on the author's page and delivered to the author's subscribers who are known as followers. Senders can restrict delivery to those in their circle of friends or allow open access. Tweets can be sent and received via the Twitter website, Short Message Service (SMS) or compatible external applications. Twitter generally contains an accessible, limited log of past messages, as well as limited user data. Twitter allows users to communicate with specific individuals or with groups.

U.S. Africa Command (AFRICOM) utilizes Twitter to communicate and engage with the public, to disseminate information, provide update on public events. For example, AFRICOM may use Twitter to provide the public with up to date and real time information about U.S. military initiatives, programs, and partnerships on the African continent, or provide period updates on the progress of long term projects. Official information posted on Twitter is also available on AFRICOM official websites. Use of Twitter also allows public affairs officials to monitor public feedback on AFRICOM activities or key issues. This can help AFRICOM dispel misinformation and help the public gain a better understanding of AFRICOM mission and related activities at the Command.

All official FTC Twitter accounts are verified by Twitter (as indicated by the blue check mark on account profiles), documented in the federal government's Social Media Registry, and also linked from the agency's Social Media web page.

All AFRICOM Twitter profiles are public, so anyone, including visitors who are not registered Twitter users, can visit the accounts and read or follow the agency's tweets. In contrast, only registered users can post tweets on Twitter. Tweets from other users do not show up in AFRICOM's home streams unless retweeted by a AFRICOM account.

If a registered user posts a tweet that includes AFRICOM's account handle, this is called a mention. The tweet will appear in the user's profile and home stream as well as the timelines of all followers of that user. Additionally, that tweet will show up in the notifications/ mentions stream of the FTC account.

If a user posts a tweet that starts with a mention of a specific AFRICOM Twitter account (e.g., @USAfricaCommand, it will only show up in the home streams of users who follow both that user and the AFRICOM account. However, all public tweets (when an account is not locked or protected) are searchable by the public on Twitter's website (or other third party sites linked to Twitter), thus anyone can search for mentions of the AFRICOM Twitter account.

Public tweets may also be picked up by search engines (e.g., Bing, Google, Yahoo!), aggregator sites, or applications outside of Twitter. AFRICOM cannot delete tweets sent by other users even if they mention a AFRICOM account, but AFRICOM can block Twitter users or

other messages that are deemed to be violent, harassing or threatening toward the Command or Command staff. Additionally, "spam" style Twitter accounts can be reported, and Twitter can investigate and delete the account if necessary.

AFRICOM may also use Twitter to promote events or answer questions in real-time.

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)*

Twitter requires users to provide their first name, last name, a valid email address, and a password, with the option to provide additional information in their biography when they register an account. Even though some of this information may be accessible to AFRICOM, depending on a Twitter user's privacy settings (users can protect their tweets by using a private account setting), AFRICOM does not routinely collect, disseminate, or maintain any of the information provided on Twitter.

However, AFRICOM may read, review, and/or rely upon information that individuals make available to the public or to AFRICOM on Twitter, as authorized or required by law. AFRICOM does not routinely use Twitter to solicit, collect, maintain, or disseminate PII from members of the public. AFRICOM may collect usernames of members of the public if messages or posts directed to AFRICOM or its employees on Twitter are deemed as threatening or violent, or where the content may reveal some other potential law enforcement violation. In addition, AFRICOM may also occasionally produce reports or summaries of its use of this social media platform that include usernames that were posted publicly if needed to comply with records retention guidelines from the National Archives and Records Administration (NARA).

AFRICOM routinely monitors keywords related to AFRICOM on Twitter and other third-party applications in an effort to determine what kind of public attention AFRICOM is generating online. AFRICOM does this manually and via automated social media management tools. Generally, comments that AFRICOM may collect or maintain as part of such review would be collected and/or maintained without the individual Twitter handle that identifies them. The Public Affairs Office may elect to include Twitter handles in the following instances:

- Twitter handles of news organizations, journalists, and influential blogs and bloggers may be collected and distributed for use in media clips to lend credibility to tweets;

- Use of Twitter handles may be collected and maintained as an official record during interactive Twitter chats or other live events hosted by the AFRICOM; and

- When answering questions directed to official AFRICOM accounts (which are verified by Twitter), AFRICOM may collect and maintain comments, including the Twitter handles of those users who posted the questions.

In the instances listed above, AFRICOM intends to keep a record of the information (generally a screen shot of the comment saved as a PDF electronically and on paper), but does not intend to collect or maintain the records in any type of database from which the records will be retrieved specifically by a Twitter handle, or any other personal identifier. The Command does not strive to collect every tweet about the agency – only tweets of significance to the Command's initiatives or missions.

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.

Twitter requires users to submit first name, last name, a valid email addresss, and a password to register a profile on the site. Individuals may choose to provide additional information in their account biography, but it is not required. AFRICOM does not collect or maintain PII that Twitter collects from registered users, particularly those who engage with AFRICOM via mentioning, following, or unfollowing of the AFRICOM account, or by participating in other activities permitted by Twitter.

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 have access to the information that Twitter collects to register for the site. AFRICOM does have access to information that users post to their public profiles. This includes name (real or pseudonym), Twitter handle, location, and any additional information they post in their biography. AFRICOM does not routinely use Twitter to solicit, collect, maintain, or disseminate PII from members of the public. In specific circumstances, AFRICOM may collect handles of members of the public (e.g., if messages or posts directed to the AFRICOM or its employees on Twitter are deemed as threatening or violent, or where the content may reveal some other potential law enforcement violation). AFRICOM may also occasionally produce reports or summaries of its use of this social media platform that include

PII posted publicly, including handles, to comply with social media records retention guidelines from the National Archives and Records Administration (NARA).

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 AFRICOM Twitter feed is not the official AFRICOM website. Twitter 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 Twitter and its application providers will adhere to the Privacy Act of 1974 or any other Federal requirement. By accessing the AFRICOM's Twitter 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, Twitter uses persistent technology throughout their sites. Users must consent to this when they accept the Twitter Terms of Service. AFRICOM may exercise limited control over the sharing of PII on its Twitter account by deleting tweets, consistent with its commenting policy, if an individual posts threatening or violent messages, or 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.	Mentions, which include username that are considered threatening or violent may be shared with agency security officials.
☐ Other DoD Components	Specify.	
☒ Other Federal Agencies	Specify.	Mentions, which include username, may be shared with NARA for records management auditing purposes. Mentions which include username, that are considered threatening or violent may be shared with Federal law enforcement.
☐ 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 AFRICOM or mentions of AFRICOM may lead to third-party, non-government websites that may have different privacy policies than those of Facebook or AFRICOM. Twitter may use persistent cookie 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 AFRICOM Twitter feed from users who interact with the command on Twitter by mentioning AFRICOM. AFRICOM routinely monitors AFRICOM-related keywords on Twitter and other third-party applications in an effort to determine what kind of public attention AFRICOM is generating online. AFRICOM does this manually and via automated social media management tools. Generally, comments that AFRICOM may collect or maintain as part of such review would be collected and/or maintained without the individual Twitter handle that identifies them.

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)*
- [ ] Official Form *(Enter Form Number(s) in the box below)*
- [ ] Paper
- [ ] Telephone Interview
- [x] Website/E-Form

As AFRICOM posts updates on its Twitter feed, individuals sometimes comment via mentions on these updates. These comments may include PII from the individual making the comment, such as their Twitter handle. Users who simply visit the AFRICOM Twitter feed and either 1) do not have a Twitter account or 2) are not logged in and/or do not interact with the page, using mentions do not make any PII available to AFRICOM Twitter 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
- [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.

Twitter is controlled and operated by a third party and is not a US government operated or managed website or application. Therefore, AFRICOM is unable to provide any assurance that the information being collected by Twitter 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.

Mentions recieved by and hashtags discovered by AFRICOM are subject to destruction when 90 days old, but longer retention is authorized if required for business use. In addition, per the AFRICOM's own privacy policy, the command does not collect any information including PII that is unnecessary. For engagement purposes on AFRICOM Twitter accounts, the command does not collect or maintain any PII beyond a Twitter handle, which minimizes potential privacy risks.

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 AFRICOM 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, USAFRICOM's use of Twitter 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	

Twitter requires users to provide their first name, last name, a valid email address, and a password, with the option to provide additional information in their biography when they register an account. Even though some of this information may be accessible to AFRICOM, depending on a Twitter user's privacy settings (users can protect their tweets by using a private account setting), the command does not routinely collect, disseminate, or maintain any of the information provided to Twitter.

Users who simply visit AFRICOM's Twitter feed and either 1) do not have a Twitter account or 2) are not logged in/do not interact with the page via mentions or the use of hashtags, do not make any PII available to AFRICOM Twitter administrators. When individuals are logged in and mention AFRICOM or hashtag certain key words, the only PII that is visible to the AFRICOM Twitter administrators is the individual's Twitter handle.

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)*

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

AFRICOM does not routinely use Twitter to solicit, collect, maintain, or disseminate PII from members of the public. Regarding the limited instances in which AFRICOM 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.

Twitter, not AFRICOM, controls the security of mentions, hash-tagged tweets or other information posted on that site. Twitter users should review Twitter'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)
- ☐ 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

Twitter controls the security of mentions, hash-tagged tweets and any other information posted on the site. Twitter users should review Twitter'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?