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:

WICKR Recall Alert and Messaging

2. DOD COMPONENT NAME:

United States Africa Command

3. PIA APPROVAL DATE:

05/24/22

AFRICOM, Components, and Subordinate Commands

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)*

- [x] 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.

WICKR Recall Alert and Messaging (RAM) is a Commercial-off-the-shelf (COTS) application product that allows users to send and receive text, chat, voice, video, and files. WICKR also allows users to send and receive Individually Identifiable Health Information (IIHI) as defined by the Health Insurance Portability and Accountability (HIPAA). WICKR RAM allows users to meet the recall, alert, and messaging (RAM) requirements of USAFRICOM, as well as DoD Cybersecurity mandates for IIHI. The WICKR application is certified for use on personal phones/tablets, government-issued phones/tablets, personal computers, government computers, or Electronic Flight Bags (EFBs). Wickr is accredited for use on mobile devices and for data up to the Impact Level 4 Controlled Unclassified Information (CUI). WICKR is maintained on the Air Force Special Operations Command (AFSOC) AO Cloud and has accepted the Risk Assessment submitted for use of this application on personal devices. The AFRICOM instance of WICKR RAM has been approved for use on personal devices.

By design, Wickr RAM is a tool to be used on unmanaged devices. The architecture of this tool maintains a secure container for both at-rest and in-transit encryption utilizing some of the highest degree of cryptography currently available over SSL. Wickr RAM utilizes the device as a keyed unit, similar to Communications Security (COMSEC) devices with type encryption. The device, is equipped with sophisticated keys for communications that are utilized in unique encryption sets either in "rooms" when more than one individual has been invited to communicate with another user, or between two users in the case of one-on-one communication. Each room, thread, and group conversation has unique keys specifically designed to secure that particular communications thread. This sophisticated key handling is what allows for the device to be accepted by the application even if the device is not managed by AFRICOM. If a device is lost or stolen or otherwise compromised, the device can be removed from the system and effectively "zeroed out" remotely. Once this is done, the device will no longer connect to the cloud, making all past Wickr RAM communications are inaccessible, and future communications impossible. Additionally, security controls such as session re-authorization, timeouts, etcetera are enforced by the service, remotely. This remote control ensures that system governance is always in accordance with the systems Authorization to Operate, and is compliant with current and future Federal Risk and Authorization Management Program (FedRAMP) and National Industrial Security Program Operating Manual (NISPOM) Cloud computing requirements and standards.

In order to access WICKR, users must request a government-purchased license. All licenses that AFRICOM uses were purchased by the US Special Operations Command (SOCOM). SOCOM is providing access to the AFRICOM users via an agreement to use those licenses. Those licenses are administered by the ARMA Global, a subsidiary of General Dynamics. Wickr Operations Team User Account Representatives (UAR) work with potential users in Wickr RAM. To ensure that system engineers and service desk personnel directly coordinate with the user to for access, removal, account cleanup, etc. UARs function as "sponsor" and main POC for user accounts in Wickr RAM.

Once a request for an account has been received, with the applicable user data provided, the Wickr RAM System administrators vet the data that the prospective user provided against the existing data in the DoD Active Directory (AD) service to validate the user as a valid Common

Access Card (CAC) holder who is currently working for the US government. Once the user has been validated, the administrators build the new user account, and then provide the new username and temporary password to the user via an encrypted email send to the email address provided in their user data and verified in AD. Once the user receives this encrypted email with their user credentials, they can use this data to setup their Wickr client application and logon to the Wickr RAM platform.

The individual military member then uses vendor provided instructions to install the application. Username and password will be provided to user via encrypted email used to register their account. Usernames and passwords are only provided once the user's account has been approved. User's must have a DoD email address that is pulled from the DOD active directory service. Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and allows administrators to manage permissions and access to network resources using their email addresses. In order to install the application, the user must use the specific password that was provided to him or verbally at time of installation. Once the application is installed, the user must be added to specific groups by group owners in order to view bi-directional chats. For instance, for Personnel Recovery and Evacuation (PR/Evac), the moderator of the PR/Evac room in Wickr RAM must add the user by looking up and selecting their username in the client directory. Once the room moderator has added the user to the room, that individual to be able to view any data that is uploaded to that room. Since DoD email addresses are retrieved from AD, the owner of the group is also provided with the name, rank, and unit of the individual seeking access, and is able to verify if the person is medical staff. Room moderators are responsible for utilizing the client directory to screen users to ensure only applicable users have been added, and when necessary removed from rooms they control. Medical staff controls licenses for medical staff attached to this request. Non-medical personnel will not be granted access to the medical licenses and/or HIPAA information.

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)*

Mission-related use: User first and last name, email address, and EDIPI is collected to provide access to the application. IIHI is collected to enable users to provide medical care at the point of injury as a patient moves through all echelons of care, ensuring clinicians have the most up-to-date information needed to ensure proper care.

User authentication: PII is used to allow a user to authenticate to the application in order to login.

Verification: PII is used to allow UARs and engineers to identify users when they register to use the application, and to ensure that each user's messages are sent to the correct recipient.

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.

Members who are eligible for medical care may object to the collection of their data if they are conscious, their life is not at risk, and they are refusing care. Otherwise, health data that is pertinent to lifesaving activities is gathered and communicated via the WICKR RAM application between documented healthcare workers to ensure patient safety without the explicit consent of the patient.

Users may object to the provision of their PII during the registration process, but will not be able to access the Wickr RAM platform if their objection results in the inability to verify their identity or authenticate them to use the application.

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.

Members my object to the collection of specific data if they are conscious, their life is not at risk, and they are refusing care. Otherwise, all pertinent health data will be gathered and distributed in the WICKR RAM app in order to ensure patient safety.

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 [ ] Not Applicable

SOCOM requires that all users complete the SOCOM User Agreement Form in order to receive license for Wickr RAM. This registration form contains SOCOM's Privacy Act Statement. The application does not retrieve patient information using personal identifiers.

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.	Patient medical data may be provided to the AFRICOM Surgeon Command.
[X] Other DoD Components	Specify.	Patient medical data may also be provided to CENTCOM, SOCOM, TRANSCOM, and EUCOM medical components
[X] Other Federal Agencies	Specify.	Patient identity and medical data may be shared with the State Department (Embassies of Countries that the patient traverses and/or enters to receive care)
[ ] 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)*

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

In order to establish a Wickr RAM account, users must provide their full name, email address, and EDIPI, in an encrypted email to the Wickr RAM System administrators to verify their identity against the available data in active directory service. The Wickr RAM application uses information pulled from the USAFRICOM active directory service to display basic user information in the user directory (ie. email address, organization, rank),

EDIPI, Rank, Name, medical care rendered/needed, next echelon of care required may be collected as part of medical care rendered and communicated through the Wickr RAM platform. The health information communicated across the Wickr RAM platform would only be done in rooms set up in the application which pertain explicitly to the applicable medical event/organization/operation. Virtual room access is limited and controlled by room moderators who were previously approved for viewing of PHI data. This ensures that only medical users involved in the care of that specific member have access to that room and any PII that may be shared.

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

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

Data will be collected from the patient, the patient's DoD ID Card, and from existing patient medical records found in the Theater Medical Data Store or Armed Forces Health Longitudinal Technology Application (AHLTA). Records may also be collected from the following websites: Theater Medical Data Store, Joint Legacy Viewer.

Information collected from users of Wickr RAM for access to the system is collected directly from the individual via email or telephone.

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier DISA K890.15; EDHA 22

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.

While PII is required and used to gain access to the system, and Wickr RAM does maintain IIHI, the system does not retrieve information of patients using any of their personal identifiers.

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. CJCSM 5760.01A 1000-02 M; 1100-06 B; and 1100.06 C.

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

(3) Retention Instructions.

Currently, IAW WICKR RAM System Information Integrity Policy Records, and PII are stored for System life, and system audit logs are stored for 1 year. AFRICOM will open a POA&M to update the retention schedules for records maintained in WICKR to comply with the following:

Systems, services, and Resources Usage and Monitoring: Usage and monitoring data and reports including operations data, such as system event logging, log-in files, system usage files, and audit trails; reports on workload management, incident reports, and audit trails of problems and solutions; and reports on operations including summary computer usage reports, measures of benchmarks, performance indicators and critical success factors, error and exception reports, self-assessments, service delivery monitoring, and management reports; excluding records created under procedures mandated by Office of Management and Budget (OMB) Circular A-123 (Management Accountability and Control Systems) and PL 97-255, the Federal Manager's Financial Integrity Act maintained by any JS/CCMD activity.- Apply CJCSM 5760.01A, 1000-02M - Destroy/Delete 3 years after cutoff

Military Personnel Health Records: Active Duty/Reserve military personnel health records held by JS/CCMD activities. Apply CJCSM 5760.01A, 1100-06B: Return to individual/Service and apply appropriate Service disposition schedule.

Civilian Employee Medical Records: Employee Medical Folder Information reflecting outpatient medical care and treatment furnished to individual civilian employees - Apply CJCSM 5760.01A, 1100-06C: OPM is the authorized custodian of these records. Transfer and destroy these records in accordance with OPM instructions and GRS 1 item 21; reassigned employees: forward file to treatment facility of record upon request; separated or retired individuals: transfer records to servicing Civilian Personnel Office for retirement in accordance with OPM instructions and GRS 1 item 21.

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.

5 U.S.C. 301, Departmental Regulation; DoD Directive 5105.19, Defense Information Systems Agency (DISA); 10 U.S.C. Chapter 55, Medical and Dental Care; and E.O. 9397 (SSN), 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.

Per DOD Manual 8901.01 volume 2, change 2, April 19, 2017, Enclosure 1, section 2b (1), Office of Management and Budget Control Number is not applicable to WICKR RAM because this system does not collect any information from the general public.

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	

For users: Full name, professional email, DOD ID Number, professional phone number, unit assigned.

For patients: Age, Rank, Name, DOD ID Number, and any medical data required for the next echelons of medical care to render care appropriate for the patient's condition.

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.

WICKR RAM will not collect or transmit Social Security Numbers.

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

N/A - WICKR RAM will not collect or transmit Social Security Numbers.

(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".

N/A - WICKR RAM will not collect or transmit Social Security Numbers in visible or machine readable format.

(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

N/A - WICKR RAM will not collect or transmit Social Security Numbers.

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
- [x] If Other, enter the information in the box below

WICKR RAM is hosted in a government privacy Cloud instance which is authorized to host Impact Level (IL) 4 PII/PHI, Non-National Security System (NSS) Controlled Unclassified Information (CUI). Amazon Web Services is responsible for securing the Cloud per the DoD provisional FEDRAMP IL 4 authorization that was granted. Data is encrypted both at rest and while in transit. Information displayed on devices cannot be captured or otherwise stored by users, and is timed to be wiped and inaccessible after reading. The licenses currently used by USAFRICOM fall under either United States Special Operations Command (USSOCOM) or Air Combat Command until cloud certification licenses have been approved by USAFRICOM. The licenses will remain active until USAFRICOM provides a cloud solution specifically for use USAFRICOM staff. Because the licenses are owned and maintained by SOCOM, SOCOM will track and approve AFRICOM users in accordance with the SOCOM internal approval process, as stated in section 1c.

(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
- [x] If Other, enter the information in the box below

- Users must have an official government email address maintained in Active Directory.
- All access to data or modifications of access controls is audited and available for forensic analysis.
- Assured Compliance Assessment Solution (ACAS) vulnerability scans are conducted against all systems. Personnel resolve identified deficiencies in accordance with security compliance standards Information Assistance Vulnerability Alerts (IAVA) such as Time Compliance Network Order / Information Assurance Vulnerability Management (TCNO/IAVM) time lines.

(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
- [ ] 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
- [x] Least Privilege Access
- [x] User Identification and Password

- Data transmitted and stored via WICKR RAM is encrypted at rest and while in transit.
- Host Based Security System (HBSS) monitors all systems in the AFSOC Cloud.
- The applications uses a mobile application manager to assist in securing the application.
- User name and password is used to login into the application from a workstation, tablet or phone.

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

Medical Users, who need to be able to communicate PHI information on the Wickr RAM platform, must provide current DHA HIPAA Training Certificate. This information is used to compile a list of "approved" users of personal health information or that can then be utilized by room moderators within Wickr RAM to be able to screen allowed users within rooms containing PHI data.

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	676
☐	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:	9/6/2019
☐	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.

(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.