



UNCLASSIFIED

UNITED STATES AFRICA COMMAND INSTRUCTION

J033

ACI 5050.01
12 August 2020

United States Africa Command Privacy Program

References:

- a. The Privacy Act of 1974, as amended, 5 U.S.C. 552a
- b. E-Government Act of 2002, P.L. 107-347, Section 208
- c. Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource", July 27, 2016
- d. Department of Defense 5400.11-R, Department of Defense Privacy Program, May 14, 2007
- e. Department of Defense Instruction 5400.11, DoD Privacy and Civil Liberties Program, January 29, 2019

Expires: 12 August 2025

1. Purpose. The purpose of this document is to establish the United States Africa Command's (USAFRICOM) internal requirements for the establishment and functioning of the Command's privacy program and assigns responsibilities for carrying out the privacy risk management requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a (Privacy Act); E-Government Act of 2002, P.L. 107-347, and Federal Information Security Management Act, P.L. 107-347, Title III, as well as general privacy risk management for USAFRICOM. This document supplements both Department of Defense (DoD) 5400.11-R and Department of Defense Instruction (DoDI) 5400.11. Nothing in this document should be construed to supersede provisions of Federal law or DoD policy.

2. Superseded. None.

3. Applicability. The policies and procedures laid out in this document apply to Personally Identifiable Information (PII) maintained by USAFRICOM

UNCLASSIFIED

UNCLASSIFIED

ACI 5050.01
12 August 2020

personnel¹, including contractors. In this policy, the term “maintain” includes, access, collection, creation, use, maintenance, dissemination, disclosure and disposal of information.

4. The policies and procedures provided in this document apply to all personnel assigned to USAFRICOM throughout the USAFRICOM Area of Responsibility².

5. Policy.

a. To the greatest extent practicable, USAFRICOM will be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of PII.

b. USAFRICOM will seek to make public, to the extent practicable, all instruments used to analyze privacy risks created by its IT Systems, operations, programs and activities. To do this, USAFRICOM will, to extent permitted by law and DoD policy, make publicly available its approved Privacy Impact Assessments, System of Records Notices (SORN), Exemption Rules, and reports developed or created in response to oversight bodies, including OMB, the USAFRICOM and DoD Offices of the Inspector General (OIG), U.S. Congress, and the Government Accountability Office (GAO).

c. USAFRICOM will maintain no Privacy Act Systems of Records (SOR) without providing prior public notice through the publication of a System of Records Notice in the Federal Register.

d. When USAFRICOM seeks to exempt a system of records from the disclosure requirements of the Privacy Act, it will publish an Exemption Rule in the Federal Register and provide means for public comment on the proposed exemption(s).

¹ Throughout this document, the term “personnel” is used to refer to all active duty service members, paid and unpaid members of the USAFRICOM staff, to include contractors and subcontractors. When used in this document, the term “contractor” refers to the organization, its employees, and the five types of contractors defined by OMB: service providers; contractor support; Government Owned, Contractor Operated facilities (GOCO); laboratories and research centers; and management and operating contracts. For more details regarding contractors, see OMB Memorandum M-14-04.

² All recommendations and requirements contained in this policy are applicable to USAFRICOM personnel, but only to the extent that such requirements and recommendations are consistent with the expressed language contained in 10 U.S.C Sections 129, and 164. The Office of Inspector General (OIG) is not a Directorate as defined in this policy, but will issue internal policies consistent with this policy and work with the USAFRICOM Privacy and Civil Liberties Officer when consistent with OIG independence.

UNCLASSIFIED

ACI 5050.01
12 August 2020

e. USAFRICOM will provide a single, clear online privacy policy that explains the Command's privacy-related practices as they pertain to its official external website and other online activities, such as its social media pages.

f. USAFRICOM will establish and maintain comprehensive privacy and civil liberties programs that comply with all applicable statutory, regulatory, and policy requirements.

g. USAFRICOM will evaluate pertinent legislative and regulatory proposals involving the collection use, and disclosure of PII, and shall continually assess compliance with all applicable Federal privacy laws and DoD regulations and policies. All USAFRICOM offices that maintain PII will:

(1) Identify the PII for which they are responsible, and provide a report to the Privacy and Civil Liberties (PCL) Office;

(2) Comply with all existing and future Federal privacy laws, regulations, and guidance pertaining to that PII; and

(3) Conduct and submit annually, Privacy Impact Assessment reviews that will be provided to the PCL Office for review and approval. These reviews must also be conducted whenever there is a change affecting the privacy or security of the system. The PCL Office will document the measures applied to comply with Federal privacy law and regulations; and assess their adequacy, based on the sensitivity of the information maintained.

h. All USAFRICOM Directorates and Special Staff Offices must establish appropriate administrative, technical and physical safeguards to ensure that PII is protected from unauthorized access, alteration, disclosure, dissemination or destruction and that confidentiality is preserved and protected. Records containing PII shall be protected against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.

i. USAFRICOM will treat records that contain personal information that normally would be withheld under Freedom of Information Exemption Numbers 3(B), 6 and 7, chapter 3 of Reference (d) as "Controlled Unclassified Information (CUI)," and safeguard them in accordance with 32 CFR Part 2002.14(b), even if they are not actually marked "CUI".

j. USAFRICOM will ensure that all contracts in which any data containing PII in USAFRICOM custody that is maintained by contractors contain the appropriate clauses as may be required by Federal Acquisition Regulations, Defense Federal Acquisitions Regulation Supplement (DFARS) and other Federal authorities in order to ensure that the DoD and USAFRICOM data

UNCLASSIFIED

ACI 5050.01
12 August 2020

under the control of the contractor is maintained in accordance with Federal law, DoD, and USAFRICOM policy.

k. Privacy and security plans shall be continually developed and security controls implemented on all networks and filing systems that maintain PII in any form. These controls shall be implemented, as required by law or policy, to protect the confidentiality and security of all operating or filing systems, application software, and data maintained in any format from accidental or malicious disclosure, alteration or destruction, and to provide assurances to the user of the quality, integrity, and confidentiality of PII maintained by USAFRICOM. Information Technology (IT) systems used to maintain PII will implement continuous monitoring and auditing of compliance with Federal guidelines and, DoD and USAFRICOM policy.

l. The physical input and output products of USAFRICOM information systems that contain privacy-protected data, including disks, paper, flash drives or any other data storage device, will be protected against misuse and unauthorized access, unauthorized disruption, unauthorized disclosure, or unauthorized modification or destruction. No technology utilized to collect, use, or disclose PII shall erode privacy protections afforded by Federal law or DoD policy.

m. Personally Identifiable Information will be maintained in a manner that will ensure:

(1) The PII is relevant and necessary to carry out a purpose prescribed by the Secretary of Defense or required by law, regulation or Executive Order;

(2) To the greatest extent practicable, the PII is collected directly from the individual to whom it pertains;

(3) When it is not possible to collect PII directly from the individual and that information is collected from third parties, it will be verified with the subject of the record to the greatest extent practicable before any negative action is taken.

(4) The individual to whom the information pertains is provided appropriate opportunities to access and amend his or her PII.³

n. USAFRICOM will develop and implement a privacy continuous monitoring program that complies with OMB requirements and DoD policy, and that is sufficient to manage associated privacy risks. At a minimum, this program will require annual assessments of privacy controls that is sufficient

³ See DODI 5400.11-R, May 14, 2007

UNCLASSIFIED

ACI 5050.01
12 August 2020

to manage associated privacy risks. In addition, USAFRICOM will maintain an inventory of the information systems that collect, use, maintain, disclose or dispose of PII. At a minimum, this program and the inventory of information systems will require annual assessments of privacy controls.

o. USAFRICOM will keep an accurate accounting of PII disclosures as required by DoDI 5400.11-R.

p. Nothing in this policy shall prevent or impede the DoD or USAFRICOM Inspector General from performing duties pursuant to the Inspector General Act or other statutory authority.

q. The audit, review, minimization and retention, Privacy Act, and E Government Act assessment and publication portions of this policy do not apply to national security systems as defined in 44 U.S.C. § 3542.

6. Responsibilities.

a. The USAFRICOM Chief of Staff will:

(1) Serve as the Senior Component Official for Privacy as required by DoDI 5400.11.

(2) Appoint a Privacy and Civil Liberties Officer to assist with the implementation, evaluation, and administration responsibilities under the Privacy Act.

(3) Ensure that an USAFRICOM Privacy Program is developed, documented, and implemented to support privacy and risk management activities for all information systems, networks, and data that support USAFRICOM operations.

(4) Oversee and provide strategic direction for the USAFRICOM privacy and civil liberties program.

(5) Ensure employee awareness of privacy and civil liberties, and the associated responsibilities to protect them.

(6) Provide advice and information to the DoD Senior Agency Official for Privacy (SAOP) on privacy issues and civil liberties concerns within USAFRICOM.

(7) Implement the DoD Breach Response Plan, and establish USAFRICOM breach management policies.

UNCLASSIFIED

ACI 5050.01
12 August 2020

(8) Ensure adequate training and awareness is provided to USAFRICOM personnel, including contractors, on how to report, respond to, and mitigate breaches of PII.

(9) Ensure that adequate procedures are in place for the management and remediation of privacy and civil liberties complaints and alleged or actual violations.

(10) Establish an USAFRICOM program to provide employee awareness of privacy and civil liberties, as well as supervisor and senior-leader understanding of responsibilities to protect privacy and civil liberties.

(11) In accordance with DoDI 8510.01, the Senior Component Official for Privacy (SCOP) will:

(12) Review and approve the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII in accordance with Appendix F of the Committee for National Security Systems Instruction (CNSSI) Number 1253.

(13) Designate which privacy controls will be treated as program management, common, information system-specific, or hybrid privacy controls within USAFRICOM.

(14) Use the Privacy Overlay found in Attachment 6 of Appendix F of CNSSI 1253 to select privacy and security controls for information systems containing PII for every stage in the systems development life cycle.

(15) Review and approve the System Privacy Plan portion of the System Security Plan, before authorization, reauthorization, or ongoing authorization, for all USAFRICOM information systems that will maintain PII.

(16) Identify assessment methodologies and metrics to determine whether privacy controls are properly implemented, operating as intended, and sufficient to ensure compliance with privacy requirements and the management of privacy risks.

(17) Identify and maintain an inventory of High Value Assets (HVA), as defined in OMB Memorandum M-17-09, Management of High Value Assets.

(18) Coordinate with the Authorizing Official on granting authorizations to operate decisions for IT systems.

(19) Ensure that the DoD SAOP is aware of information systems and USAFRICOM Systems of Records containing PII that cannot be appropriately

UNCLASSIFIED

ACI 5050.01
12 August 2020

protected or secured; and ensure that such systems are prioritized for upgrade, replacement, or retirement.

b. The USAFRICOM Privacy and Civil Liberties Officer (PCLO) will:

(1) Manage and supervise the functions of the DoD Privacy and Civil Liberties Programs at USAFRICOM.

(2) Advise senior USAFRICOM officials on proper procedural, contractual, technical, or programmatic actions required to correct privacy-related deficiencies.

(3) Ensure appropriate administrative, physical, and technical safeguards and procedures are established for information systems that maintain PII.

(4) Develop and implement an oversight and compliance function to provide the required guidance and reviews to meet the Privacy Act, E-Government Act, and other government-wide and DoD privacy requirements.

(5) Develop and implement a privacy continuous monitoring program that complies with OMB requirements and DoD policy and that is adequate to manage associated privacy risks.

(6) Ensure corrective actions identified during privacy risk assessment activities are properly tracked and monitored until findings are corrected.

(7) Collaborate, as necessary and appropriate, with information management, information collection, information security, forms and publications management, public affairs, records management, the Command, Control, Communications, and Computer Systems (C4S), and legal counsel staffs.

(8) Work with the Information Systems Security Manager (ISSM) or equivalent designee to determine the confidentiality risk and associated mitigations of information systems, and ensure that controls intended to mitigate privacy risk are implemented and effective.

(9) To the extent authorized by the Privacy Act of 1974, use procedures of 32 CFR 310, Protection of Privacy and Access to and Amendment of Individual Records Under the Privacy Act of 1974.

(10) Process requests from individuals for access to records or information pertaining to themselves maintained in a System of Records, and provide that information to the individual unless it can be properly withheld under one or more applicable Privacy Act exemptions. An acknowledgement

UNCLASSIFIED

ACI 5050.01
12 August 2020

will be provided to the individual within 10 days (excluding Saturdays, Sundays, and legal public holidays).

(11) Pursuant to a request from the individual, correcting or amending records pertaining to them maintained in a System of Records in accordance with the Privacy Act, if USAFRICOM determines that the records are not accurate, relevant, timely, or complete. If an amendment request is denied, and the individual appeals the denial, processing the denial.

(12) Implement, consistent with guidance and processes established by the DPCLTD and this policy, the process for the completion, review, tracking and approval of privacy compliance and risk management strategies, and documents including, but not limited to, Privacy Impact Assessment (PIA), and System of Records Notices (SORN).

(13) Submit SORNs and any applicable exemption rules to DPCLTD for review and publication.

(14) Implement formal breach management policies and procedures, and provide training to personnel, including contractors, about how to report and respond to breaches of PII.

(15) Provide mechanisms for the submission of privacy and civil liberties complaints and alleged violations in accordance with DoD 5400.11-R.

(16) Ensure that personnel, including contractors, are aware of methods to address allegations of privacy and civil liberties violations.

(17) Coordinate with USAFRICOM personnel, as appropriate, to complete a DD Form 2930, Privacy Impact Assessment (PIA), for every USAFRICOM IT system and electronic collection that maintains or will maintain information about members of the public, DoD personnel, contractors, or foreign nationals employed at U.S. military facilities internationally, in accordance with DoDI 5400.16, PIA Instructions, and submit the final PIA to DPCLTD for review.

(18) Work with the USAFRICOM Public Affairs Office (PAO) to ensure that PIAs are available on the USAFRICOM public website for as long as a system, program, or electronic collection maintains PII, in accordance with OMB Policy and DoDI 5400, and ensuring that data that raises security concerns or reveals sensitive or classified data are not made publicly available.

(19) Coordinate with the USAFRICOM PAO to ensure that all USAFRICOM websites include a consistent USAFRICOM online privacy policy that complies with Office of Management and Budget and Department of Defense requirements.

UNCLASSIFIED

ACI 5050.01
12 August 2020

(20) Coordinate with System Owners to maintain a compilation of systems that access, collect, create, use, maintain, disseminate, disclose or dispose of PII.

(21) Ensure that the link from the Department of Defense Chief, Information Officer (DoD CIO) PIA website to the USAFRICOM PIA is maintained by emailing new and updated URLs to osd.mcalex.dod-cio.mbx.pia@mail.mil.

(22) Ensure that an electronic copy of the final, signed PIA is submitted the DoD CIO by emailing it to osd.mcalex.dod-cio.mbx.pia@mail.mil.

(23) Work with individual system owner, program owners, and C4S Systems management to review PIAs for systems and electronic collections on an annual basis to ensure that they are accurate.

(24) Update PIAs for systems and electronic collections triennially or when there is a significant change to its privacy or security posture, whichever occurs first.

(25) Ensure the Insider Threat Program officials are provided privacy and civil liberties training, and ensuring that their training programs operate in accordance with DoDD 5205.16.

(26) Coordinate with the USAFRICOM Office of Legal Counsel on privacy training, incident response activities, and publication of SORN and SORN exemption rules.

c. The USAFRICOM Senior Information Systems Security Officer will:

(1) Work with Program and System Owners to ensure that System Security Plans are completed and that all System Security Plans for systems that maintain PII include a System Privacy plan.

(2) Evaluate the sensitivity of any PII accessed, created, used or retained in the information system.

d. The USAFRICOM Office of Legal Counsel will consult with the USAFRICOM PCLO to:

(1) Identify laws, regulations, and internal policies that apply to PII and provide guidance of their impact and implementation requirements.

(2) Provide information to the USAFRICOM PCLO to help identify proposed programs or regulations that may create privacy risk.

UNCLASSIFIED

ACI 5050.01
12 August 2020

(3) Interpret statutory language to ensure that USAFRICOM collections of PII are appropriately authorized.

(4) Participate in drafting of privacy notices (e.g., PIAs and SORNS), information collections, and rulemakings.

e. USAFRICOM Program Owners will:

(1) Ensure that resources are requested and appropriately applied to identify, evaluate, and mitigate privacy risk associated with a service, activity, or IT system.

(2) Communicate operational requirements for the maintenance of PII to the USAFRICOM PCLO during the privacy risk assessment (e.g., PIA) process and prior to the collection or use of PII.

(3) Ensure that operations use information consistent with the published PIA, SORN, and exemption rules, and notify USAFRICOM PCLO if any proposed use or change of use is not explicitly covered by any of these notices.

(4) Coordinate with System Owner to inventory information systems that access, collect, create, use, maintain, disseminate, disclose or dispose of PII and provide information about these systems to the PCLO upon request

(5) Notify the USAFRICOM PCLO when establishing, making significant changes or decommissioning an IT system that maintains PII.

(6) Keep an accurate accounting of all disclosures of PII to all external entities and provide the list to the PCLO upon request. If a record is amended pursuant to the Privacy Act, provide the entities with which the information was shared with the updated information.

(7) Begin the PIA process when a new IT system that will collect, store, or process identifiable information is proposed; when starting to significantly modify an existing information system; or when a new electronic collection of identifiable information is being proposed.

(8) Collaborate with the USAFRICOM PCLO to draft a SORN for each new, significantly altered and terminated system of records throughout the lifecycle of the system.

(9) Collaborate with System Owners to ensure all privacy regulatory compliance reporting is entered and updated as required by DoD policy.

f. System Owners will:

UNCLASSIFIED

ACI 5050.01
12 August 2020

(1) Ensure that the information system is operated in accordance with the applicable privacy controls, as identified by the USAFRICOM PCLO and ISSM.

(2) Monitor and immediately report any suspected actual unauthorized alteration, disclosure, or destruction of PII to the Information Assurance Team and the USAFRICOM PCLO.

(3) Ensure that proper measures are taken to maintain the confidentiality of PII in all IT systems for which they are responsible.

(4) Coordinate with Program Owner to inventory information systems that access, collect, create, use, maintain, disseminate, disclose or dispose of PII and provide information about these systems to the PCLO upon request.

g. USAFRICOM Contracting Officers or Contracting Officer Representatives will:

(1) Coordinate with the System Owners, Business Owners, Project Officers/Managers and USAFRICOM PCLO to ensure that the appropriate privacy risk management language from the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS), Procedures, Guidance, and Information (PGI), and other relevant sources is incorporated into all contracts.

(2) Work with the System Owners, Business Owners, Project Officers/Managers, Legal Counsel, and the USAFRICOM PCLO to ensure that contractual privacy risk management obligations are upheld.

(3) Coordinate with the USAFRICOM PCLO regarding deliverable acceptance, and reject deliverables that create privacy risk or do not meet privacy obligations as defined in this policy, FAR, DFARS, and/or contracts.

(4) Report actual or suspected privacy-related incidents, including PII breaches and violations by contracted personnel or contracted parties, to the USAFRICOM PCLO and in a manner consistent with the USAFRICOM Privacy Breach Management Policy.

(5) Ensure that any remediation directed at contracted personnel or contracted parties for PII breaches or violations is implemented.

h. USAFRICOM Personnel will:

(1) Access records containing PII of others only when needed to carry out their official duties.

UNCLASSIFIED

ACI 5050.01
12 August 2020

(2) Disclose PII about others in accordance with applicable Federal privacy laws, DoD regulations as policies, and USAFRICOM policies and procedures.

(3) Report all suspected and actual unauthorized collection, use, maintenance, dissemination and deletion of PII.

(4) Participate in training and awareness programs on privacy and data protection policies, information privacy laws, regulations, DoD and USAFRICOM policies and procedures to promote awareness and compliance.

(5) Sign and agree to rules of behavior, establishing their responsibilities for the protection of PII.

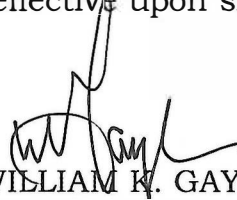
7. Additional Paragraphs: Additional Paragraphs may be added as determined by the OPR.

8. Summary of Changes. None.

9. Releasability.

Unclassified Unlimited. This directive is approved for public release; distribution is unlimited. Users may obtain copies on the USAFRICOM network portal.

10. Effective Date. This instruction is effective upon signature.



WILLIAM K. GAYLER
Major General, U.S. Army
Chief of Staff, U.S. Africa Command

Enclosure(s):

A. Acronyms, Abbreviations, and Terms

UNCLASSIFIED

ACI 5050.01
12 August 2020

Enclosure A

Acronyms, Abbreviations, and Terms

1. Acronyms/Abbreviations

ACI - Africa Command Instruction
CFR – Code of Federal Regulations
CIO – Chief Information Officer
CNSSI –Committee of national Security Systems Instruction
CUI –Controlled Unclassified Numbers
C4S – Command, Control, Communications, and Computer Systems
DFARS –Defense Federal Acquisition Regulation Supplement
DPCLTD –Defense Privacy, Civil Liberties, and Transparency Division
DoD - Department of Defense
DoD CIO – Department of Defense Chief Information Officer
DoDD – Department of Defense Directive
DoDI – Department of Defense Instruction
FAR –Federal Acquisition Regulation
FIPS – Federal Information processing Standard
FOUO – For Official Use Only
GAO – Government Accountability Office
HVA – High Value Asset
ISSM –Information Systems Security Manager
IT –Information Technology
MOU/A – Memorandum of Understanding or Agreement
NARA –National Archives and Records Administration
NIST –National Institute of Standards and Technology
OE –Other Equipment
OIG – Office of Inspector General
OMB – Office of management and Budget
OPR – Office of Primary Responsibility
ISSO – Information Systems Security Officer
PAO – Public Affairs Office
PCL –Privacy and Civil Liberties Office
PCLO – Privacy and Civil Liberties Officer
PGI –Procedures, Guidance, and Information
PIA – Privacy Impact Assessment
PII – Personally Identifiable Information
SAOP – Senior Agency Official for Privacy
SCOP – Senior Component Official for Privacy
SPII – Sensitive Personally Identifiable Information
SOR – System of Records
SORN – System of Records Notice

A-1

UNCLASSIFIED

UNCLASSIFIED

ACI 5050.01
12 August 2020

SSN – Social Security Number
USAFRICOM - U.S. Africa Command

2. Terms

Access. For the purposes of this USAFRICOM policy, the review of a record or a copy of a record, or parts thereof, in a system of records by any individual.

Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than those authorized, for another than authorized purpose, have access or potential access to personally identifiable information.

Civil Liberties. Fundamental rights and freedoms protected by the Constitution of the United States of America.⁴

Complaint. An assertion alleging a violation of an individual’s legal right to privacy or a violation of civil liberties.⁵

Individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual may also act on behalf of an individual. Members of the U.S. Armed Forces are “individuals. Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not “individuals” whether acting in an entrepreneurial capacity with the Department of Defense, but are “individuals” when acting in a personal capacity (e.g., security clearances, entitlement to DoD privileges or benefits, etc.).⁶

Information Life Cycle. The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.⁷

IT System. Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by

⁴ See DoDI 5400.11, January 29, 2019

⁵ ID

⁶ See DoD 5400.11-R, May 14 2007

⁷ OMB Circular A-130, Managing Information as a Strategic Resource, July 2016

UNCLASSIFIED

ACI 5050.01
12 August 2020

the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.⁸

Interagency Agreement. A written agreement entered into between two or more Federal agencies that specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other(s) (the requesting agency), including assisted acquisitions as described in OMB Memorandum: Improving the Management and Use of Interagency Acquisitions and other cases described in *Federal Acquisitions Regulation* (FAR) Part 17.

Maintain. For purposes of this USAFRICOM policy, maintain means to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

National Security System. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy (44 U.S.C. § 3552).

Official Use. This term is used when officials and employees of a DoD Component have demonstrated a need for the use of any record or the information contained therein in the performance of their official duties, subject to DoD 5200.1-R.⁹

⁸ ID

⁹ See DoD 5400.11-R, May 14 2007

UNCLASSIFIED

ACI 5050.01
12 August 2020

Personally Identifiable Information. Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.¹⁰

Privacy and Civil Liberties Officer (PCLO). A federal employee who is responsible for the day-to-day management of the DoD Component privacy and civil liberties programs.¹¹

Privacy Continuous Monitoring Strategy. A formal document that catalogues the available privacy controls implemented at an agency across the agency risk management tiers and ensures the controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.¹²

Privacy Control. The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and to manage privacy risks.

Privacy Impact Analysis (PIA). An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate the protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.¹³

Privacy Plan. A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting the applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls. This document may be integrated into the system security plan, as appropriate.

Privacy Program Plan. A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the

¹⁰ OMB Circular A-130, Managing Information as a Strategic Resource, July 2016

¹¹ DoD 5400.11-R, May 14 2007

¹² OMB Circular A-130, Managing Information as a Strategic Resource, July 2016

¹³ ID

UNCLASSIFIED

ACI 5050.01
12 August 2020

strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting the applicable privacy requirements and managing privacy risks.¹⁴

Program Owner. The champion of the service, activity, or information systems, and owner of the requirement for the service, activity or system.

Record. Any item, collection, or grouping of information, whatever the storage media (paper, electronic, etc.), about an individual that is maintained by a DoD Component, including, but not limited to, an individual's education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph.¹⁵

Record Disposition. A comprehensive term that includes destruction as well as other actions, such as the transfer of permanent records to the National Archives. After appraising agency records, NARA authorizes either their disposal or their transfer to the National Archives for preservation and research.¹⁶

Risk. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Routine Use. The disclosure of a record outside the Department of Defense for a use that is compatible with the purpose for which the information was collected and maintained by the Department of Defense. The routine use must be included in the published system notice for the system of records involved.¹⁷

Security Control. The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.¹⁸

Senior Component Official for Privacy (SCOP). A member of the Senior Executive Service, a Senior Level Employee, or a general officer or flag officer

¹⁴ ID

¹⁵ See DoD 5400.11-R, May 14 2007

¹⁶ See National Archives and Records Administration Records Disposition Overview

¹⁷ DoD 5400.11-R, May 14 2007

¹⁸ OMB Circular A-130, Managing Information as a Strategic Resource, July 2016

UNCLASSIFIED

ACI 5050.01
12 August 2020

responsible for the overall implementation of the privacy and civil liberties programs in his or her DoD Component.¹⁹

System of Records. A group of records under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual.²⁰

System of Records Notice (SORN). The notice(s) published by an agency in the *Federal Register* upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN is comprised of the Federal Register notice(s) that identified the system of records, the purpose of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom the records are maintained, the routine uses to which the records are subject, and additional details about the system as described in the Office of Management and Budget (OMB) *Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*. As explained in the Circular, a SORN may be comprised of a single *Federal Register* notice addressing all of the required elements that describe the current system of records, or it may be comprised of multiple *Federal Register* notices that together address all of the required elements.²¹

System Owner. The key point of contact (POC) for the information system who is responsible for coordinating System Development Life Cycle activities specific to the IT system.

¹⁹ DoDI 5400.11, January 29, 2019

²⁰ DoD 5400.11-R, May 14 2007

²¹ See OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.

Enclosure B

U.S. Africa Command's Fair Information Practice Principles

1. Transparency

a. To the greatest extent practicable, USAFRICOM will be transparent and provide notice to individuals regarding its collection, use, dissemination, and maintenance of PII.

b. USAFRICOM will seek to make public, to the extent practicable, all instruments used to analyze privacy risks created by its IT Systems, operations, programs and activities. To do this, USAFRICOM will, to extent permitted by law and DoD policy, make publicly available its approved Privacy Impact Assessments, System of Records Notices (SORN), Exemption Rules, and reports developed or created in response to oversight bodies, including OMB, the USAFRICOM and DoD Offices of the Inspectors General (OIG), U.S. Congress, and the Government Accountability Office (GAO).

c. USAFRICOM will maintain no SORNs without providing prior public notice through the publication of a System of Records Notice in the Federal Register.

d. When USAFRICOM seeks to exempt a system of records from the disclosure requirements of the Privacy Act, it will publish an Exemption Rule in the Federal Register and provide means for public comment on the proposed exemption(s).

e. USAFRICOM will provide a single, clear online privacy policy that explains the Command's privacy-related practices as they pertain to its official external website and other online activities, such as its social media pages.

2. Individual Participation and Redress

a. To the extent practicable, USAFRICOM will seek consent for its collection, use, maintenance, and dissemination of PII. When such collection may result in the determination of rights and privileges under Federal law, USAFRICOM will make reasonable efforts to collect information directly from the individual to whom it pertains.

b. USAFRICOM will seek consent from the individual before using information for any new purposes not disclosed at the time it was collected.

UNCLASSIFIED

ACI 5050.01
12 August 2020

c. USAFRICOM will provide a mechanism for receiving and responding to individual's complaints, concerns, and questions about its privacy practices.

d. USAFRICOM will provide appropriate access, correction, and redress for its uses of PII.

3. Authority and Purpose Specification

a. Prior to collection, USAFRICOM will determine the legal authority that permits its collection, maintenance, use, and dissemination of PII and limit such activities to those permitted by law. These activities will also be limited to those that support a specific programmatic or administrative need.

b. USAFRICOM will maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute, by the individual to whom the record pertains, or unless pertinent to and within the scope of an authorized law enforcement activity.

c. Unless explicitly authorized or required by law, USAFRICOM will permit the internal sharing of PII only for purposes that are compatible with the original purpose for which the PII was collected, and as specified at that time.

4. Data Minimization and Retention

a. USAFRICOM will collect only information about individuals that is relevant and necessary for the performance of agency mission or to accomplish a purpose required by statute, DoD Regulation or an Executive Order of the President.

b. USAFRICOM will periodically review its PII holdings, focusing on Social Security numbers (SSN), to determine if continued collection is authorized, necessary, and appropriate and will eliminate unnecessary holdings.

c. Subject to DoD requirements, USAFRICOM will not collect or use SSNs as personal identifiers in connection with any information system or database, unless the collection and/or use is authorized and provided for by law. Where SSN collection and/or use is authorized, USAFRICOM will make reasonable attempts to substitute other identifying information in the place of SSNs.

d. When collecting SSNs, USAFRICOM will notify the individual whether the provision of the SSN is mandatory or voluntary, as defined in the Privacy Act. USAFRICOM will also provide the specific the statutory or regulatory authority for the collection, and advise the individual from whom it is collected, how the SSN will be used.

B-2

UNCLASSIFIED

UNCLASSIFIED

ACI 5050.01
12 August 2020

e. USAFRICOM will not deny an individual any right, benefit, or privilege as a result of refusing to provide their SSN, unless the collection is required by law or authorized either by statute or by a regulation issued prior to 1975.²²

f. USAFRICOM will ensure that records displaying PII, regardless of the storage medium, are disposed of in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule and in a manner that prevents loss, theft, misuse or unauthorized access.

5. Use Limitation

a. Prior to sharing any Privacy Act data, USAFRICOM will ensure that the recipient organization affords the equivalent or better level of administrative, physical, and technical security controls as when maintained by USAFRICOM.

b. USAFRICOM will document all authorized external sharing of PII via an Memorandum of Understanding/Agreement (MOU/A) or other approved instrument that explicitly defines the purpose, conditions and authorized use of shared information in connection with an authorized law enforcement activity under Section 552a(b)(7) of the Privacy Act.

c. Prior to participating in any computer matching activity USAFRICOM will ensure that it has been approved by the Defense Data Integrity Board, and that a notice of the matching activity has been published in the Federal Register.

6. Data Quality and Integrity

a. USAFRICOM will make reasonable efforts, prior to disseminating a record about an individual, to ensure that the record is accurate, relevant, timely and complete.

b. USAFRICOM will develop and implement reasonable procedures to ensure the accuracy of the data shared and of any data received from external sources.

c. If inaccuracies are discovered in data that has been shared, USAFRICOM will make reasonable efforts to ensure that the corrected data is provided to the entity with which it was shared. In the case of PII, a written request will be made for the recipient to correct or delete it.

²² See The Privacy Act of 1974, as amended, 5 U.S.C. 552a

7. Security

- a. USAFRICOM will protect PII from risks such as loss; unauthorized access, use, destruction or modification; or unintended or inappropriate disclosure through the use of appropriate security safeguards.
 - b. All PII will be protected using administrative, physical, and technical security controls consistent with DoD “CUI” processes. PII processed and stored electronically will be protected consistent with Federal Information Processing Standard (FIPS) 199 moderate security standards.
 - c. The USAFRICOM Privacy and Civil Liberties Office (PCL Office) may, in accordance with OMB Circular A-130, Managing Information as a Technical Resource, Appendix B; OMB Memorandum; and FIPS 199, increase or decrease the accepted confidentiality risk of PII in a particular information system on a case-by-case basis, based on a determination about the risk of reasonably anticipated threats that could result in harm to individuals or to the Command as result of unauthorized use or disclosure of PII.
 - d. USAFRICOM will implement encryption protections, using only DoD-authorized National Institute of Standards and Technology (NIST)-certified cryptographic modules, for all electronic Sensitive PII that is transported and/or stored offsite unless otherwise authorized, in writing, by the Senior Component Official for Privacy.
- PII will be stored only on DoD-issued computers, tablets, and other mobile devices.
- e. USAFRICOM will require all personnel who maintain Sensitive PII (SPII) on mobile computing devices or who work off-site at any time and have access to SPII to certify that SPII will be properly safeguarded against loss or compromise.
 - f. USAFRICOM will develop and implement a Privacy Incident Response Plan that provides an organized and effective response to privacy incidents.
 - g. USAFRICOM will ensure that all personnel are provided with a clear definition of what constitutes a breach involving PII and are aware of how, where and what information is needed to report the actual or suspected loss, inappropriate access, use or sharing of PII.

8. Accountability and Auditing

UNCLASSIFIED

ACI 5050.01
12 August 2020

a. USAFRICOM will establish a Command-wide Privacy Program, managed by the USAFRICOM PCLO, accountable for complying with this policy and all applicable Federal privacy protection requirements by developing, disseminating and implementing privacy policies and procedures that establish the appropriate privacy controls for programs, information systems or technologies.

b. USAFRICOM will establish a privacy training program and ensure that all personnel who maintain or access PII in any medium, including contractors, receive privacy training prior to being granted access to any DoD or USAFRICOM record containing the PII of others.

c. USAFRICOM will ensure that all personnel involved in the design, development, operation, maintenance or control of any system of records, including contractors, are informed of all requirements to protect the privacy of the individuals whose information is contained in the records and sign a Privacy Rules of Behavior Acknowledgement.

d. USAFRICOM will include appropriate privacy provisions in all contracts and other acquisition-related documents for USAFRICOM systems that contain PII if they are developed, maintained, operated, or managed by contractors.

e. USAFRICOM will obtain written assurance from third parties who work on official USAFRICOM or DoD business that said third party will protect PII in a manner consistent with this DoD and USAFRICOM policy during all phases of the information lifecycle.

f. USAFRICOM will hold all personnel accountable for compliance with the standards laid forth in this ACI.

UNCLASSIFIED

ACI 5050.01
12 August 2020

Enclosure C

U.S. Africa Command's Rules of Behavior

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including sensitive information, or information systems of the U.S. Africa Command (USAFRICOM).

1. GENERAL RULES OF BEHAVIOR

a. I understand that when I use any Government information system, I have no expectation of Privacy in records that I create or in my activities while accessing or using such information system.

b. I understand that authorized DoD and USAFRICOM personnel may review my conduct or actions concerning DoD or USAFRICOM information and information systems, and take appropriate action. Authorized USAFRICOM personnel include my supervisory chain of command as well as USAFRICOM and DOD system administrators and Information Systems Security Officers (ISSOs). Appropriate action may include monitoring, recording, copying, inspecting, restricting access, blocking, tracking, and disclosing information to authorized Office of Inspector General (OIG), DoD, USAFRICOM, and Federal law enforcement personnel.

c. I understand that the following actions are prohibited: unauthorized access, unauthorized uploading, unauthorized downloading, unauthorized changing, unauthorized circumventing, or unauthorized deleting information on DoD systems, unauthorized modification of DoD systems, unauthorized denying or granting access to DoD systems, using DoD resources for unauthorized use on DoD systems, or otherwise misusing DoD systems or resources. I also understand that attempting to engage in any of these unauthorized actions is also prohibited.

d. I understand that such unauthorized attempts or acts may result in disciplinary or other adverse action, as well as criminal, civil, and/or administrative penalties. Depending on the severity of the violation, disciplinary or adverse action consequences may include appropriate criminal prosecution, civil judicial action, disciplinary or adverse administrative action, a court-martial under the Uniform Code of Military Justice, or other administrative action authorized by U.S.C. or Federal regulations. Theft, conversion, or unauthorized disposal or destruction of Federal property or information may also result in criminal sanctions.

C-1

UNCLASSIFIED

UNCLASSIFIED

ACI 5050.01
12 August 2020

e. I understand that I have a responsibility to report suspected or identified information security and/or privacy incidents to my supervisor and the Information Assurance Team.

f. I understand that I have a duty to report information about actual or possible criminal violations involving DoD and USAFRICOM programs, operations, facilities, contracts or information systems to my supervisor, any management official or directly to the OIG, including reporting to the OIG Hotline. I also understand that I have a duty to immediately report to the OIG any possible criminal matters involving felonies, including crimes involving information systems.

g. I understand that the USAFRICOM Rules of Behavior do not and should not be relied upon to create any other right or benefit, substantive or procedural, enforceable by law, by a party to litigation with the United States Government.

h. I understand that the USAFRICOM Rules of Behavior do not supersede any policies that provide higher levels of protection to USAFRICOM's information or information systems. The USAFRICOM Rules of Behavior provide the minimal rules with which individual users must comply.

i. I understand that if I refuse to sign the USAFRICOM Rules of Behavior as required by USAFRICOM policy, I may be denied access to DoD and USAFRICOM information and information systems. Any refusal to sign the USAFRICOM Rules of Behavior may have an adverse impact on my deployment or assignment to USAFRICOM, or employment with USAFRICOM.

2. SPECIFIC RULES OF BEHAVIOR.

a. I will follow established procedures for requesting access to any DoD or USAFRICOM computer system and for notification to my supervisor and the USAFRICOM Office of Security Management when the access is no longer needed.

b. I will follow established USAFRICOM information security and privacy policies and procedures.

c. I will use only devices, systems, software, and data which I am authorized to use, including complying with any software licensing or copyright restrictions. This includes downloads of software offered as free trials, shareware or public domain.

UNCLASSIFIED

ACI 5050.01
12 August 2020

d. I will only use my access for authorized and official duties, and to only access data that is needed in the fulfillment of my duties as provided for in DoD 5500.7-R, Joint Ethics Regulation.

e. I will secure sensitive information in all areas (at work and remotely) and in any form (e.g. digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all sensitive information must be in a protected environment at all times or it must be encrypted (using DoD-provided, FIPS 140-2 approved encryption). If clarification is needed whether or not an environment is adequately protected, I will follow the guidance of the USAFRICOM.

f. I will properly dispose of sensitive information, either in hardcopy, softcopy or electronic format, in accordance with DoD and USAFRICOM policy and procedures.

g. I will not attempt to override, circumvent or disable operational, technical, or management security controls unless expressly directed to do so in writing by authorized USAFRICOM or DoD staff.

h. I will not attempt to alter the security configuration of government equipment unless authorized. This includes operational, technical, or management security controls.

i. I will protect my verify codes and passwords from unauthorized use and disclosure and ensure I utilize only passwords that meet the DoD minimum requirements for the systems that I am authorized to use.

j. I will not store any passwords/verify codes in any type of script file or cache on DOD or USAFRICOM systems.

k. I will ensure that I log off or lock any computer before walking away and will not allow another user to access that computer while I am logged on to it.

l. I will not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any DoD or USAFRICOM electronic communication system.

m. I will not auto-forward e-mail messages to addresses outside the DoD network.

n. I will comply with any directions from my supervisors, DoD or USAFRICOM system administrators and information security officers concerning my access to, and use of, DoD and USAFRICOM information and information systems or matters covered by these Rules.

UNCLASSIFIED

ACI 5050.01
12 August 2020

o. I will ensure that any devices that I use to transmit, access, and store sensitive information outside of a DoD-authorized, protected environment will use FIPS 140-2 approved encryption (the translation of data into a form that is unintelligible without a deciphering mechanism). This includes laptops, tablets, mobile devices, thumb drives, and other removable storage devices and storage media (CDs, DVDs, etc.).

p. I will obtain the approval of appropriate management officials before releasing USAFRICOM information for public dissemination.

q. I will not host, set up, administer, or operate any type of Internet server on any DoD network or attempt to connect any personal equipment to a DoD network unless explicitly authorized in writing by the Director of C4S Systems and I will ensure that all such activity is in compliance with Federal, DoD and USAFRICOM policies.

r. I will not attempt to probe computer systems to exploit system controls or access sensitive data for any reason other than in the performance of official duties. Authorized penetration testing must be approved in writing by the Director of C4S Systems.

s. I will protect Government property from theft, loss, destruction, or misuse. I will follow DoD and USAFRICOM policies and procedures for handling Federal Government IT equipment and will sign for items provided to me for my exclusive use and return them when no longer required for USAFRICOM activities.

t. I will only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by DoD on USAFRICOM equipment or on computer systems that are connected to any DoD network.

u. If authorized, by waiver, to use my own personal equipment, I must use DoD-approved virus protection software, anti-spyware, and firewall/intrusion detection software, and ensure that the software is configured to meet DoD and USAFRICOM configuration requirements. The USAFRICOM C4S Cybersecurity and Strategy Division will confirm that the system meets USAFRICOM configuration requirements prior to connection to DoD's network.

v. I will never swap or surrender USAFRICOM hard drives or other storage devices to anyone other than an authorized C4S employee at the time of system problems.

w. I will not disable or degrade software programs used by the USAFRICOM that install security software updates to USAFRICOM computer equipment, to

UNCLASSIFIED

ACI 5050.01
12 August 2020

computer equipment used to connect to DoD information systems, or to create, store or use DoD information.

x. I agree to allow examination by authorized C4S personnel of any personal IT device [Other Equipment (OE)] that I have been granted permission to use, whether remotely or in any setting to access USAFRICOM information or DoD or USAFRICOM information systems or to create, store or use USAFRICOM information.

y. I agree to have all equipment scanned by the C4S Cybersecurity and Strategy Division prior to connecting to the VA network if the equipment has not been connected to the DoD/USAFRICOM network for a period of more than three weeks.

z. I will complete mandatory periodic security and privacy awareness training within designated timeframes, and complete any additional required training for the particular systems to which I require access.

aa. I understand that if I must sign a non-USAFRICOM entity's Rules of Behavior to obtain access to information or information systems controlled by that non-USAFRICOM entity, I still must comply with my responsibilities under the USAFRICOM Rules of Behavior when accessing or using USAFRICOM information or information systems. However, those Rules of Behavior apply to my access to, or use of the non-USAFRICOM entity's information and information systems as an USAFRICOM user.

bb. I understand that remote access is allowed from other Federal government computers and systems to DoD or USAFRICOM information systems, subject to the terms of both USAFRICOM's and the host Federal agency's policies.

cc. I agree that I will directly connect to the DoD/USAFRICOM network whenever possible. If a direct connection to the network is not possible, then I will use USAFRICOM-approved remote access software and services. I must use USAFRICOM-provided IT equipment for remote access when possible. I may be permitted to use non-USAFRICOM IT equipment [Other Equipment (OE)] only if a C4S Director-approved waiver has been issued and the equipment is configured to follow all DoD and USAFRICOM security policies and requirements. I agree that C4S and Office of Security Management officials may examine such devices, including an OE device operating under an approved waiver, at any time for proper configuration and unauthorized storage of sensitive information.

UNCLASSIFIED

ACI 5050.01
12 August 2020

dd. I agree that I will not have both a DoD/USAFRICOM network connection and any kind of non-DoD/USAFRICOM network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by C4S Cybersecurity and Strategy Division.

ee. I agree that I will not allow sensitive information to reside on non-DoD or non-USAFRICOM systems or devices unless specifically designated and approved in advance by the appropriate USAFRICOM official (supervisor), and a waiver has been issued by the Director of C4S Systems. I agree that I will not access, transmit or store remotely any sensitive information that is not encrypted using DoD-approved encryption.

ff. I will obtain my USAFRICOM supervisor's authorization, in writing, prior to transporting, transmitting, accessing, and using sensitive information outside of DoD's or USAFRICOM's protected environment.

gg. I will ensure that sensitive information, in any format, and devices, systems and/or software that contain such information or that I use to access sensitive information or information systems are adequately secured in remote locations, e.g., at home and during travel, and agree to periodic inspections of the devices, systems or software from which I conduct access from remote locations. I agree that I will work with sensitive information from a remote location pursuant to an approved telework agreement and with the approval of my first-level supervisor.

hh. I will protect sensitive information from unauthorized disclosure, use, modification, or destruction, including using encryption products approved and provided by USAFRICOM to protect sensitive data.

ii. I will not store or transport any sensitive information on any portable storage media or device unless it is encrypted using DoD-approved encryption.

jj. I will use DoD-provided encryption to encrypt any e-mail, including attachments to the email that contains sensitive/FOUO information before sending the e-mail. I will not send any email that contains sensitive information in an unencrypted form. Sensitive information includes personally identifiable information and protected health information.

kk. I may be required to acknowledge or sign additional specific or unique rules of behavior in order to access or use specific DoD and USAFRICOM systems. I understand that those specific rules of behavior may include, but are not limited to, restrictions or prohibitions on limited personal use, special requirements for access or use of the data in that system, special requirements

UNCLASSIFIED

ACI 5050.01
12 August 2020

for the devices used to access that specific system, or special restrictions on interconnections between that system and other IT resources or systems.

3. Acknowledgement and Acceptance

- a. I acknowledge that I have received a copy of these Rules of Behavior.
- b. I understand, accept and agree to comply with all terms and conditions of these Rules of Behavior.

[Print or type your full name] Signature

Date

Office Phone

Position Title

C-7

UNCLASSIFIED