UNITED STATES AFRICA COMMAND MANUAL

J033

ACM 5050.02
30 September 2020

Privacy Incident Response

References:

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

b. OMB Memorandum 17-12, Preparing and Responding to a Breach of Personally Identifiable Information.

c. DoD 5400.11-R, Department of Defense Privacy Program, May 14, 2007.

d. DoD Instruction 5400.11, DoD Privacy and Civil Liberties Program, January 21, 2019.

e. ACI 3200.14, U.S. Africa Command Privacy Risk Management, 31 July 2020.

Expires: 18 September 2025

1. Purpose. This manual provides Headquarters, United States Africa Command (USAFRICOM), its subordinate Components, and Agencies, who participate in or provide services to USAFRICOM, throughout the Area of Responsibility, with overarching guidance for responding to incidents involving personal information. This instruction provides policy and establishes responsibilities and processes for organizations within USAFRICOM and its subordinate Components, and Agencies.

2. Superseded. None.

3. Applicability. This manual applies to known or suspected incidents that involve the actual or potential unauthorized access, use, or disclosure of Personally Identifiable Information (PII) or other personal information maintained by USAFRICOM personnel regardless of medium on which it occurs. In this policy, the term "maintain" includes the collection, creation, use, maintenance, and dissemination of information. The procedures provided in this section apply to all personnel assigned to USAFRICOM throughout the USAFRICOM Area of Responsibility.

4. Policy. The goal of Privacy Incident Management is to synchronize Privacy Incident Response efforts for USAFRICOM, its Components and Agencies. This instruction establishes the framework to ensure the Commander, United States Africa Command is provided, by the most efficient means; privacy incident detection, analysis, containment, remediation, reporting, and where possible, proactive mitigation. Also, this instruction ensures that organizations and personnel who provide those services maintain a thorough understanding of required privacy incident response activities, and processes.

5. Responsibilities. All users of USAFRICOM information are responsible for the protection of PII and other personal information. This document focuses on establishing the Incident Response roles and responsibilities of the following: USAFRICOM Privacy and Civil Liberties Office, USAFRICOM Cybersecurity, Law Enforcement and Counter-Intelligence agencies (LE/CI), and users of USAFRICOM information.

6. Summary of Changes. None.

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

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

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

Enclosures:
A. Acronyms, Abbreviations, and Terms
B. Privacy Incident Responsibilities
C. Privacy Incident Response Training Requirements
D. Categorization and Remediation of Electronic Events Involving PII
E. Breach Report Template
F. Breach Exploitation Risk Measurement Methodology
G. Factors Influencing Risk Level
H. Sample Breach Notification Letter

Enclosure A

1. Acronyms/Abbreviations

AOR – Area of Responsibility
AR - Army Regulation
C4S - Command Control, Communications and Computer Systems
CART - Compliance and Reporting Management Tool
COS – Chief of Staff
CSSP – Cyber Security Service Provider
DLP – Data Loss Prevention
DoD – Department of Defense
DPCLTD – Defense Privacy Civil Liberties and Transparency Division
ISSM – Information System Security Manager
IT – Information Technology
LE/CI – Law Enforcement and Counter Intelligence
NDCI – Negligent Disclosure of Classified Information
NIST – National Institute of Standards and Technology
OIG – Office of the Inspector General
OLC – Office of Legal Counsel
OMB – Office of Management and Budget
OSD – Office of the Secretary of Defense
OSM – Office of Security Management
PB – Privacy Breach
PCLO – Privacy and Civil Liberties Officer
PII – Personally Identifiable Information
PIN – Personal Identification Number
PV – Privacy Violation
SSN – Social Security Number
USAFRICOM – United States Africa Command

2. Terms

Breach - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses PII for any other than authorized purpose.[1]

[1] OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally-Identifiable Information, January 3, 2017

Breach Response Plan - An agency's formal document that includes the policies and procedures that must be followed with respect to reporting, investigating, and managing a breach.[2]

Breach Response Team - The group of agency officials designated by the head of the agency that the agency must convene to respond to a breach.[3]

Federal Information System - Any information system used or operated by an agency, by a contractor, or by another agency on behalf of an agency.[4]

High Risk - Any organizational (e.g. Directorate or Staff Office) compilation of electronic records containing PII of 500 or more individuals stored on a single device or accessible through a single application or service, regardless of whether or not the compilation is subject to the Privacy Act of 1974.

Identify Theft - The use of another person's PII (e.g., name, Social Security number, credit card number) without permission and used to commit fraud or any other crime.

Information Owner - Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.[5]

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 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. IT system 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. IT system does not include any

[2] ID

[3] ID

[4] OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016

[5] NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations

equipment that is acquired by a contractor incidental to a contract which does not require its use.[6]

Misuse - The act of a user or IT system utilizing PII in a manner other than that which was originally intended and authorized.

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.

Privacy Incident - An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

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.[7]

Senior Component Official for Privacy - The senior official designated by the head of the Component who has Component-wide responsibility for privacy, including implementation of privacy protections, compliance with federal laws, regulations, and policies relating to privacy; management of privacy risks at the component, and a central policy-making role in the Component's development and evaluation of legislative, regulatory, and other policy proposals.

Unauthorized Access - The act of a user or a system gaining access to PII without proper authorization.

Unauthorized Disclosure - The act of a system or user providing, releasing, or making available PII without appropriate authorization.

Unauthorized Modification - The act of a system or use changing PII.

USAFRICOM Information - Information created, collected, processed, maintained, disseminated, disclosed, or disposed by or on behalf of the United States Africa Command in any medium or form.

[6] See OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016

[7] See OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016

Enclosure B

Privacy Incident Responsibilities

1. Internal Organization Responsibilities. USAFRICOM Privacy and Civil Liberties Officer (PCLO) has the responsibility to ensure Privacy Incident Response Management occurs according to referenced Office of Management and Budget (OMB) Guidelines and DoD instructions.

a. USAFRICOM Chief of Staff (COS) will:

(1) In consultation with the PCLO, the Office of Legal Counsel (OLC), and the C4 Systems Directorate (J6), determine whether or not individuals will receive written notification of a breach that has been determined to be high risk.

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

(1) Accept reports from USAFRICOM J6 detailing potential PII incidents.

(2) Determine when a reported PII incident creates a violation of the Privacy Act of 1974, OMB Guidelines, and/or DoD regulatory requirements.

(3) Provide the J6 ISSM with written guidance for determining the remediation efforts required to fully address incidents.

(4) Work with the J6 ISSM to implement remediation measures, as appropriate.

(5) Use information provided by J6 to submit an interim incident report, to include the associated the ticket number, to the Office of the Secretary of Defense (OSD) Defense Privacy Civil Liberties and Transparency Division (DPLCTD) using the DPCLTD Compliance and Reporting Management Tool (CART)

(6) For incidents involving any USAFRICOM information system, the PCLO will:

(a) Within 5 workdays of receiving a report of a privacy event, work with J6 to determine whether the incident reaches the threshold of a "high risk" breach.

1 If the event is determined to be high risk, the PCLO will work with J6 to determine to whom the PII involved belongs, as it may be necessary to inform these individuals within 10 business days of discovery.

2 Consult with the J6 and the COS in the event that Command Control, Communications and Computer Systems (C4S) Directorate is unable to determine likelihood of a breach using Appendix C, for a determination of risk.

(b) If the PCLO determines that it is possible and necessary to provide notification of the breach, although the breach does not meet the criteria of a "high risk" event, the PCLO, in consultation with the OLC and J6, will coordinate production of the notifications and provide them to the affected individuals within 10 business days of the discovery of the breach. If J6 intends to provide notification of a privacy breach to the affected individuals, the Privacy Office must be notified at least one day before notice is provided.

(c) Ensure that any investigation of a breach determined to be high risk follows Army Regulation (AR) 15-6 procedures and:

1 Provide a report of the high risk incident, based on information obtained from the Interim Incident Report, and any other details provided by the J6. This report will be provided to the Chief of Staff, and DPCLTD by the end of the second day following the discovery of the breach.

2 If the breach involves government credit card information, ensure that the issuing bank is notified at the same time that the affected individuals are notified.

(d) For a breach that does not meet the "high risk" threshold, the PCLO, in coordination with J6, will determine if it is necessary to notify the USAFRICOM Office of the Inspector General (OIG). If it is determined that an investigation is warranted, the result of the investigation will be provided to the USAFRICOM COS for disposition.

(7) For incidents not involving information systems:

(a) Conduct an investigation into the cause in order to ensure that the condition that led to the breach has been contained.

(b) Direct actions, in accordance with 32 CFR 310, DoD Privacy Program to mitigate the harm that could result from a breach. This may include:

1 Requesting that the Office of Security Management seize and secure records, and;

2 Requesting that records be reviewed for retention compliance by the USAFRICOM Records Officer.

(c) Closing event tickets that are reported to J6 as a breach of PII. Commented.

(8) Submitting a copy of the Final Incident Report to DPCLTD. A copy will also be sent to J6 and Operations and Plans Division (J63) with a request to close the incident ticket. USAFRICOM J63 will notify U.S.-CERT of the final disposition of the incident.

c. USAFRICOM Command, Control, Communications, and Computer Systems (C4S) (J6) will:

(1) Identify policy violations based on Cyber Security Service Provider (CSSP) generated incident reports and develop incident packages when applicable for investigative purposes.

(2) Assist with exceptions to policy by coordinating privacy threat/risk assessments within USAFRICOM assets.

(3) Provide a copy all incident description with privacy implications to the PCLO.

(4) Notify the PCLO and Office of Security Management (OSM) within one hour of any electronic breach involving PII or other personal information.

(5) For incidents involving electronic breaches:

(a) Respond to PCLO requests for information about privacy incidents and assist in their investigation when personal information is the subject of a potential incident.

(b) Provide to the USAFRICOM PCLO and the Office of Security Management, the facts surrounding the incident, to include the type(s) of PII involved, actions taken in response to the breach, number and type(s) of individuals whose PII was involved (e.g., Military, DoD Civilian, Members of the Public, Dependents, etc.), and the number of people who accessed the PII.

(c) Provide a Technical Assessment of complicated breaches based on the facts surrounding the incident, and assign a likelihood determination level as defined in Appendix F of this document.

(d) Continue to report in accordance with DoD policy until the underlying cause of the breach has been resolved.

(e) If J6 determines that the incident is unusually complicated, in addition to the process listed above in (b), provide a technical assessment of the situation.

(6) The J6 ISSM will manage Personally Identifiable Information (PII) incidents in direct coordination with the USAFRICOM Information Security Information Security and Privacy Officers, respectively, and will:

(a) Authorize account disablement and deletion based on incident severity, user non-compliance, and data retention requirements.

(b) Coordinate remediation efforts with all applicable organizations as defined and directed by PCLO.

(7) Receive briefings from the CSSP on significant privacy-related cyber incidents affecting the USAFRICOM Area of Responsibility (AOR).

(8) Provide command visibility of significant privacy incidents in order to direct corrective/remediation actions against threats to information on USAFRICOM networks.

(9) Make a Technical Assessment as to the likelihood that the PII has been accessed, by how many personnel, and if possible, by whom, and for how long; and the technical and data details pertaining to the breach.

(10) Provide a Technical Assessment of complicated breaches based on the facts surrounding the incident, and assign a likelihood determination level as defined in Appendix C of this document.

(11) Work with external entities to ensure that the underlying cause of the breach has been contained.

(12) Continue to report in accordance with DoD policy until the underlying cause of the breach has been resolved.

(13) Obtain additional information and data concerning cyber incidents, obtain points of contact for further investigation purposes, or in regards to reclassification or reprioritization of incidents.

(a) If containment of the underlying cause for the breach requires disabling or disconnecting an information system, before proceeding, J63 and system manager must receive approval from the J6 Director. The J6 Director may, as deemed necessary, consult with the USAFRICOM Commander and Information Owner prior to disabling or disconnecting an IT system.

(b) After obtaining the J6 Director's approval, the J63 will disable or disconnect the information system and then notify the USAFRICOM PCLO, Chief of Staff, the Information Owner, and OLC.

(14) Brief Command leadership and effect coordination with Law Enforcement and Counter-Intelligence (LE/CI) assets supporting the Command, when appropriate, if a privacy-related cyber-incident occurs.

d. USAFRICOM Information Security Officer will:

(1) Accept reports detailing potential privacy incidents.

(2) Determine when a reported privacy incident meets the criterion of a Negligent Disclosure of Classified Information (NDCI).

(3) Define the scope and extent of all NDCI circumstances and provide the J6 ISSM with written guidance detailing the extent of remediation efforts required to fully address the incident.

(4) Ensure the affected system is secured as outlined for information system users, and open a "Category: Privacy" trouble ticket.

(5) Immediately notify the supporting Signal unit of the situation, and take no additional actions to investigate the system or events until directed by CSSP.

(6) Provide timely response to cyber pertaining to USAFRICOM.

(7) Assist in mitigation measures as required by J6.

(8) Comply with the Privileged Level User Account Access Policy.

e. USAFRICOM Office of Legal Counsel will:

(1) Accept notification of confirmed breaches from PCLO.

(2) Provide legal opinions about whether breach notification is required, and the sufficiency of breach notification communications.

(3) Coordinate with PCLO on the production of breach notification communications within 10 days of the discovery of a confirmed breach.

f. USAFRICOM Users will:

(1) In the event of a suspected privacy incident, the user will immediately notify the local security manager and workgroup administrator. Users must also support and be responsive to guidance and direction from the J6, PCLO, and the INFOSEC Officer.

(a) If possible, ensure that the information is secured.

(b) Collect as many details about the event as possible. (e.g., what information was involved, what were the circumstances, and how did the event take place or how was the event discovered?).

(c) Create a "Category: Privacy" trouble ticket using the "119" ticketing system either telephonically via DSN 119 of Commercial Line +49 (0)61-1143-523-1000 or online using the 119 desktop icon within one hour of the discovery of the event.

(2) Report any activities, indicators, and behaviors as potential threats to personal information including events involving Insider Threat and CI.

Enclosure C

Privacy Incident Response Training Requirements

1. All Users.

a. All users accessing USAFRICOM IT Systems are required to attend an initial Information Assurance and the Cyber Threat Briefing when in-processing to the combatant command. These topics are briefed at the USAFRICOM Newcomer's Orientation Course.

b. All users must successfully complete the DoD Cyber Awareness Challenge to gain and maintain authorization to access USAFRICOM IT systems. The DoD Cyber Awareness Challenge is an annual training requirement.

c. All users must successfully complete JS-US002, Joint Staff Privacy Act Awareness to gain and maintain access to PII or the equivalent USAFRICOM Privacy Awareness training. This is an annual training requirement.

2. USAFRICOM PCLO personnel:

a. At a minimum PCLO personnel will be trained to investigate and analyze all response activities related to privacy events. These tasks include, but are not limited to: incident reporting, creating and maintaining incident tracking information; planning, coordinating, and directing recovery activities; and incident analysis tasks, including examining all available information and supporting evidence or artifacts related to an event.

b. Per DoDI 5400.11 PLCO staff will be trained to implement the DoD Breach Response Plan.

Enclosure D

Categorization and Remediation of Electronic Events Involving PII

TABLE 1. PII Event Categorization

PII Event Type	Nature of Event	
	Deliberate Act*	Inadvertent Act**
Unauthorized Access (A)	AD	AI
Unauthorized Disclosure (D)	DD	DI
Unauthorized Modification (M)	MD	MI
Misuse (U)	UD	UI
Mishandling (H)	HD	HI
Not a PII Incident (N)	ND	NI

*Deliberate Act	An intentional action demonstrating "a lack of attention, care, or concern" for safeguarding PII in accordance with USAFRICOM or DoD requirements. E.g., A user emails a list that includes SSNs of USAFRICOM personnel to a member of the public.
**Inadvertent Act	An action demonstrating a prudent and reasonable effort to comply with USAFRICOM and DoD requirements for safeguarding PII; however, the action constitutes a violation of policy. E.g., A user places an unencrypted document that includes Names and SSNs of USAFRICOM personnel on a shared drive that is accessible only to their team. Each team member who has access has a need to know the information to perform her or his official duties.

TABLE 2. PII Mitigation Category, based on PII Event Category[8]

	PII EVENT CATEGORY				
	NI or NN	HI	AI or HD	UD, UI or DD, DI	AD or MD, MI
PII Remediation Category	NI or NN	PV	PI	PI/PB[9],[10]	PB

[8] NOTE. A PII event may fit into more than one PII Event Category. For example, a file placed on shared drive that is able to be accessed by numerous people, some with and some without a need to know, may fit into both the HD and HI categories. HI because some users had a need to know, but HD because some users did not. In accordance with NIST guidance on incident categorization, the incident should be categorized according to the highest event category that applies. For instance, the event described above would be considered HD.

[9] Misuse event (U) type PII remediation will depend on the outcome of the technical (and other) investigation.

[10] Unauthorized disclosure (D) type PII remediation will depend on the outcome of the technical investigation. E.g., Was the transmission internal or external, and were those who received it authorized?

Table 3. PII Mitigation Category Description and Mitigation Requirements[11]

PII Mitigation Category	Example	Mitigation Required
Not a PII Incident (NI or NN)	An employee sends his own, unencrypted PII from his USAFRICOM computer c: drive email account to his personal email is not a PII incident. While this is not a good security practice, the employee may send his own PII however he chooses. Similarly, if an USAFRICOM employee stores her own unencrypted PII on a shared drive, it is a poor security practice, does not constitute an incident. If DLP were to detect unencrypted PII being stored or sent via an USAFRICOM network, it is to be considered a PV. As more is learned about the nature of the information, the mitigation categorization may change.	None.

[11] OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017, requires agencies to develop and implement a breach response plan that includes the agency's policies and procedures for reporting, investigating, and managing a breach, and it should be specifically tailored to the agency and address the agency's missions, size, structure, and functions. The breach response plan must assess and mitigate the risk of harm to individuals potentially affected by a breach.

Policy Violation (PV)	A policy violation will have occurred, when PII is kept on a USAFRICOM internal system with access controls (e.g., PII on an organizational shared drive or SharePoint site where access controls limit access to only a limited number of personnel such as administrative assistants, team members, or other members of a cognizable group within the internal organization.) The number of personnel with access to the PII is typically less than 25 internal users, although contributing factors such as clearance and responsibility of the users along with sensitivity of the data can result in increases or decreases to this number based on an assessment of these contributing factors. NOTE: To be a PV, the shared drive must not have global access permissions. This would allow anyone who accesses the shared drive would	However, the PCLO and OSM should be notified. First, determine if the file containing the PII has a named USAFRICOM user as owner and not the "Administrator," or "System" account – either of which indicates an "ownerless" file under Windows File Management. If the file has either the "Administrator" or "System" owner, "move the file to secure location" and leave a marker in the directory informing users that this file contained PII and has been quarantined. If the file has a named USAFRICOM user as owner, and it has not been modified in the past 2 years, "move the file to secure location" and leave a marker in the directory informing that user that this file contained PII and has been quarantined. Access for named users will be restored with a request from their supervisor authorizing their access. When returned, the user should be informed of the requirement to password protect or encrypt the file. If the file has a named USAFRICOM user as owner and it has been modified in

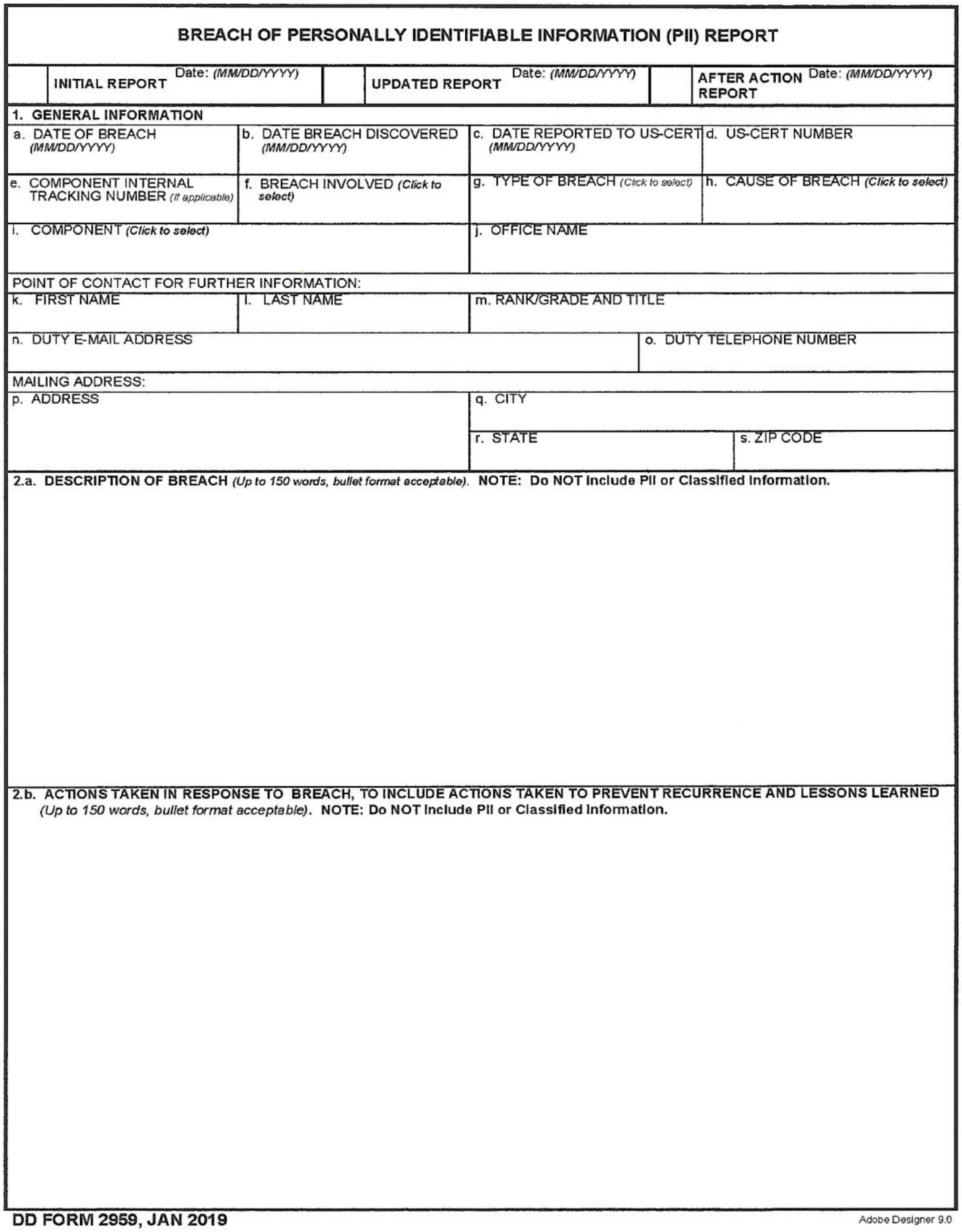
	have access to the PII, increasing the mitigation category.	the past 2 years, the remediator will flag the event for the file as containing PII using the DLP tool. These events will be tracked and reported as part of the overall DLP scanning program status as the Privacy Act requires audit and accountability.
PII Incident (PI)	PII stored on USAFRICOM internal system that does not utilize access controls (or only uses generic domain access controls, e.g., access controls limited to all Users) or PII transmitted across public switches to other Federal agencies without using encryption. Both incidents will require investigation to determine if a PB has occurred or whether it remains a PII Incident.	Events meeting criteria for PII Incidents will be managed in accordance with the requirements of this document, starting at Paragraph 6. Such events will be treated as suspected breaches of PII until the investigative process described in paragraph 8b and forward in the above document determines otherwise and will be escalated to DPCLTD. If, after the investigative process is complete, the event is determined to not be a breach the determination will be forwarded to the PCLO so that the ticket can be closed out. If a breach is determined to have occurred that involves NDCI, it must be reported to

🟨		The USAFRICOM Office of Security Management for tracking, and Privacy Office for reporting, tracking, investigation, and remediation. Employee discipline or contractual actions may be required and proper chain of evidence and incident tracking is required. NOTE: If after investigation, it is later determined the event does not meet PB criteria, then the IA Team may record the event as a PII Incident (if appropriate) and DoD and United States Computer Emergency Readiness Team (US CERT) notification.

PII Breach (PB)	PII stored or transmitted on/to an external system that does not have requisite DoD-level security controls. Examples include, but are not limited to: 1) sending unencrypted email containing PII to another Federal agency or a personal email account; 2) posting unencrypted documents containing PII on the Internet. A "PII Incident" becomes a "PB" when the loss of either the security, integrity, or both, of the PII could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual on whom the information is maintained.	Events meeting criteria for PBs will be managed in accordance this document, beginning at paragraph 6, and will be escalated to the J6 and the Office of Security Management for reporting and tracking, and to the Privacy Office US CERT notification will be required. Employee discipline or contractual actions may be necessary and proper chain of evidence and incident tracking is required.

Enclosure E

DD Form 2959, Breach Report Template



BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT

□	**INITIAL REPORT** Date: *(MM/DD/YYYY)*	□	**UPDATED REPORT** Date: *(MM/DD/YYYY)*	□	**AFTER ACTION REPORT** Date: *(MM/DD/YYYY)*

1. GENERAL INFORMATION

a. DATE OF BREACH *(MM/DD/YYYY)*	b. DATE BREACH DISCOVERED *(MM/DD/YYYY)*	c. DATE REPORTED TO US-CERT *(MM/DD/YYYY)*	d. US-CERT NUMBER
e. COMPONENT INTERNAL TRACKING NUMBER *(If applicable)*	f. BREACH INVOLVED *(Click to select)*	g. TYPE OF BREACH *(Click to select)*	h. CAUSE OF BREACH *(Click to select)*
i. COMPONENT *(Click to select)*		j. OFFICE NAME	

POINT OF CONTACT FOR FURTHER INFORMATION:

k. FIRST NAME	l. LAST NAME	m. RANK/GRADE AND TITLE
n. DUTY E-MAIL ADDRESS		o. DUTY TELEPHONE NUMBER

MAILING ADDRESS:

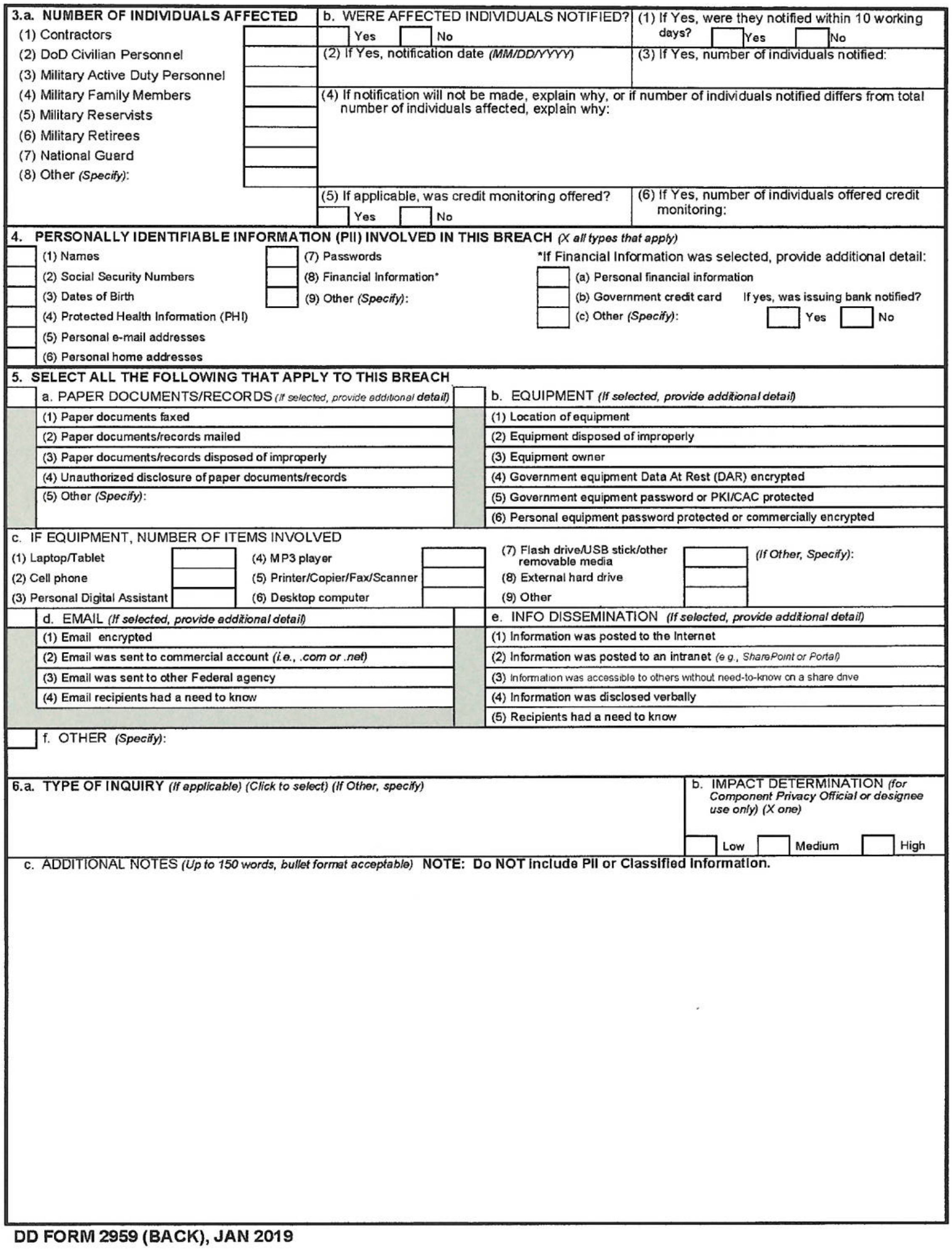
p. ADDRESS	q. CITY	
	r. STATE	s. ZIP CODE

2.a. **DESCRIPTION OF BREACH** *(Up to 150 words, bullet format acceptable).* **NOTE: Do NOT include PII or Classified Information.**

2.b. **ACTIONS TAKEN IN RESPONSE TO BREACH, TO INCLUDE ACTIONS TAKEN TO PREVENT RECURRENCE AND LESSONS LEARNED** *(Up to 150 words, bullet format acceptable).* **NOTE: Do NOT include PII or Classified Information.**

DD FORM 2959, JAN 2019

Adobe Designer 9.0



3.a. NUMBER OF INDIVIDUALS AFFECTED

(1) Contractors □
(2) DoD Civilian Personnel □
(3) Military Active Duty Personnel □
(4) Military Family Members □
(5) Military Reservists □
(6) Military Retirees □
(7) National Guard □
(8) Other *(Specify)*: □

b. WERE AFFECTED INDIVIDUALS NOTIFIED? □ Yes □ No

(1) If Yes, were they notified within 10 working days? □ Yes □ No

(2) If Yes, notification date *(MM/DD/YYYY)*

(3) If Yes, number of individuals notified:

(4) If notification will not be made, explain why, or if number of individuals notified differs from total number of individuals affected, explain why:

(5) If applicable, was credit monitoring offered? □ Yes □ No

(6) If Yes, number of individuals offered credit monitoring:

4. PERSONALLY IDENTIFIABLE INFORMATION (PII) INVOLVED IN THIS BREACH *(X all types that apply)*

□ (1) Names
□ (2) Social Security Numbers
□ (3) Dates of Birth
□ (4) Protected Health Information (PHI)
□ (5) Personal e-mail addresses
□ (6) Personal home addresses
□ (7) Passwords
□ (8) Financial Information*
□ (9) Other *(Specify)*:

*If Financial Information was selected, provide additional detail:
□ (a) Personal financial information
□ (b) Government credit card   If yes, was issuing bank notified? □ Yes □ No
□ (c) Other *(Specify)*:

5. SELECT ALL THE FOLLOWING THAT APPLY TO THIS BREACH

□ a. PAPER DOCUMENTS/RECORDS *(If selected, provide additional detail)*
(1) Paper documents faxed
(2) Paper documents/records mailed
(3) Paper documents/records disposed of improperly
(4) Unauthorized disclosure of paper documents/records
(5) Other *(Specify)*:

□ b. EQUIPMENT *(If selected, provide additional detail)*
(1) Location of equipment
(2) Equipment disposed of improperly
(3) Equipment owner
(4) Government equipment Data At Rest (DAR) encrypted
(5) Government equipment password or PKI/CAC protected
(6) Personal equipment password protected or commercially encrypted

c. IF EQUIPMENT, NUMBER OF ITEMS INVOLVED

(1) Laptop/Tablet	□	(4) MP3 player	□	(7) Flash drive/USB stick/other removable media	□	*(If Other, Specify)*:
(2) Cell phone	□	(5) Printer/Copier/Fax/Scanner	□	(8) External hard drive	□	
(3) Personal Digital Assistant	□	(6) Desktop computer	□	(9) Other	□	

□ d. EMAIL *(If selected, provide additional detail)*
(1) Email encrypted
(2) Email was sent to commercial account *(i.e., .com or .net)*
(3) Email was sent to other Federal agency
(4) Email recipients had a need to know

□ e. INFO DISSEMINATION *(If selected, provide additional detail)*
(1) Information was posted to the Internet
(2) Information was posted to an intranet *(e.g., SharePoint or Portal)*
(3) Information was accessible to others without need-to-know on a share drive
(4) Information was disclosed verbally
(5) Recipients had a need to know

□ f. OTHER *(Specify)*:

6.a. TYPE OF INQUIRY *(If applicable) (Click to select) (If Other, specify)*

b. IMPACT DETERMINATION *(for Component Privacy Official or designee use only) (X one)*
□ Low □ Medium □ High

c. ADDITIONAL NOTES *(Up to 150 words, bullet format acceptable)* **NOTE: Do NOT include PII or Classified Information.**

DD FORM 2959 (BACK), JAN 2019

Enclosure F

Breach Exploitation Risk Methodology

Based on National Institute of Standards and Technology (NIST) Special Publication 800-30

1. Likelihood Determination (Step 1):

a. To derive an overall likelihood rating that indicates the probability that a potential breach/vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

(1) Motivation and capability of threat source; and

(2) Existence and effectiveness of current controls.

b. The likelihood that a potential breach/vulnerability could be exploited by a given threat source can be described as very high, high, medium, low, or very low.

Table 1.1. Definitions of Likelihood

Likelihood Rating	**Definition**
Very High	The threat source has a very sophisticated level of expertise, is very well resourced, and seeks to undermine, severely impede, or destroy a core mission, business function; or program by targeting specific employees or positions, infrastructure providers/suppliers, or partnering organizations. The vulnerability is exposed and exploitable (security controls not implemented and not planned or no security measure can be identified to remediate the vulnerability).
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exploited are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the breach/ vulnerability
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the breach/vulnerability from being exercised.

Very Low	The threat-source has been all but eliminated as having either motivation or capability either through forensics or through direct query.

2. Impact Analysis (Step 2):

a. The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a breach/vulnerability. Before beginning the impact analysis, it is necessary to obtain the following information about data sensitivity.

b. Information about data sensitivity can be obtained from existing organizational documentation, such as the asset criticality assessment report. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets that support the organization's critical missions.

c. An asset criticality report or similar document does not exist, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners, in consultation with J6, are responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).

d. The adverse impact of an event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence(s) for its forfeiture:

(1) Loss of Integrity. System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality.

(2) Loss of Availability. If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the mission.

(3) Loss of Confidentiality. System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security (high risk) to the disclosure of Privacy Act data or PII (low risk). Unauthorized, unanticipated, or unintentional disclosure could result in loss if public or personnel confidence, embarrassment, or legal action against the Command.

e. Some tangible impacts can be measured quantitatively in loss of time to devote to mission, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of confidence, lost opportunities, loss of credibility, and damage to organizational interests) cannot be measured in specific units but can be qualified or described in terms of high, moderate, and low impacts. This guide describes only the qualitative categories—high, medium, and low impact (see Table 2.1).

f. In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments.

(1) The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a true cost-benefit analysis of any recommended controls difficult.

(2) The major advantage of a quantitative impact analysis is that it allows the organization to measurement of the magnitude of the impact. That can then be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to:

(a) An estimation of the frequency of the threat-source's exercise of the breach/vulnerability over a specified time period (e.g., 1 year).

(b) An approximate cost for each occurrence of the threat-source's exercise of the breach/vulnerability.

(c) A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific breach/vulnerability.

g. The desired output from Impact Analysis is to determine the magnitude of impact. Magnitude determinations are categorized as either high, medium, or low.

Table 2.1. Impact Magnitude Categories

Magnitude of Impact	Definition
High	Exploitation of the breach/vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly harm or impede an organization's mission; (3) may significantly harm or violate an organization's or individual's reputation or interest; or (4) may result in human death or serious injury.
Moderate	Exploitation of the breach/vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may harm or impede an organization's mission; (3) may harm or violate an organization's or individual's reputation or interest; or (4) may result in human injury.
Low	Exploitation of the breach/vulnerability (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an organization's mission; (3) may noticeably affect an organization's or individual's reputation or interest.

3. Risk Determination (Step 3). The purpose of this step is to assess the level of risk to the IT system containing the PII. The determination of risk for a particular threat/breach/vulnerability pair can be expressed as a function of:

a. The likelihood of a given threat-source's attempting to exercise a given breach/vulnerability.

b. The magnitude of the impact should a threat-source successfully exercise the breach/vulnerability.

c. The adequacy of planned or existing security controls for reducing or eliminating risk.

2. To measure risk, a risk scale and a risk-level matrix must be developed. The final determination of risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 3.1 below shows how the overall risk ratings will be determined based on inputs from the threat likelihood and threat impact categories.

3. The matrix in Table 3.1 shows how the overall risk levels of “Very High, High, Medium, Low, and Very Low” are derived. The determination of these

risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. The probability assigned for each threat likelihood level is 1.0 for Very High, 0.80 for High, 0.5 for Medium, 0.1 for Low, 0.01 for Very Low. For example:

> *If the level indicated on certain items is so low as to be deemed to be "negligible" or non-significant (value is <0.01), they can be put aside in a separate bucket in lieu of forwarding for management action. This will make sure that they are not overlooked when conducting the next periodic risk assessment. It also establishes a complete record of all risks identified in the analysis. These risks may be moved to a new risk-level on a reassessment due to a change in threat likelihood and/or impact and that is why it is important that they be accounted for in the exercise.*

4. Consult with the J62 and the Chief of Staff in the event that J6 is unable to determine likelihood of a breach using Section 1.1, for a determination of risk. If the risk level is determined to be at least "high", in accordance with Table 3.1, the affected individuals must be notified.

Table 3.1. Risk Level Assessment Matrix

The values assigned the impact levels are **100** for High, **50** for Moderate, and **10** for Low.

Threat Likelihood	Impact		
	Low (10)	Moderate (50)	High (100)
Very High (1.0)	10x1=**10**	50x1=**50**	100x1= **100**
High (.66)	10x.66=**6.6**	50x.66=**33**	100x.66=**66**
Medium (.35)	10x.35=**3.5**	50x.35=**17.5**	100x.35=**35**
Low (.10)	10x.1=**1**	50x.1=**5**	100x.1=**10**
Very Low (.01)	10x.01=**.1**	5.x.01=**.5**	100x.01=**1**

Table 3.2. Actions Corresponding to Risk Level

Risk Level	Requisite Action
High (50 or above)	If an observation or finding is evaluated as a high risk, affected individuals are required to be notified.
Moderate (17.5-49)	If an observation is rated as medium risk, affected individuals may be required to be notified. J6 must contact USAFRICOM Privacy Office to discuss the results of this risk assessment and what next steps should be taken.
Very Low or Low (.1-17.4)	If an observation or event is described as low, individuals are not required to be notified. The likely harm is so low that notification will not be a benefit them and may result in falsely alarming them.

Enclosure G

Factors Influencing Risk Level:

1. Data Elements.

a. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. For example:

> *The theft of a database containing individuals' names in conjunction with Social Security numbers, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.*

b. It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context.

> *For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher risk of harm, whereas a database of names of subscribers to agency media alerts may pose a lower risk of harm.*

c. In assessing the levels of risk of harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

2. Number of Individuals Affected**.** The magnitude of the number of affected individuals may dictate the method(s) you choose for providing notification, but should not be the determining factor for whether an agency should provide notification.

3. Information Accessibility/Usability.

a. Upon learning of a breach, the organization should assess the likelihood PII will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the agency's decision to provide notification.

b. The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. However, this will depend upon a number of physical, technological, and procedural safeguards employed. If the information is properly protected by NISTvalidated encryption, for example, the risk of compromise may be low to non-existent.

c. Agencies will first need to assess whether the PII is at a low, moderate, or high risk of being compromised. The assessment should be guided by NIST security standards and guidance (see Enclosure F for USAFRICOM Implementation). Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.

4. Likelihood of Harm.

a. Section 5 U.S.C. § 552a (e)(10) of the Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Possible harms associated with the loss or compromise of information must be considered. In addition to potential financial harm, harms may include the effect of a breach of confidentiality or fiduciary responsibility, augmented potential for blackmail through the disclosure of private facts resulting in mental pain and emotional distress. They also include the potential disclosure of address information for victims of abuse, as well as the potential for secondary uses that could result in fear or uncertainty, humiliation, or loss of self-esteem.

b. The likelihood of harm will depend on the data involved in the breach. Social Security numbers with names and dates of birth are of particular concern due to their value for committing identity theft. However, they are not the only data elements of particular concern. Information such as medical diagnoses, names or addresses of witnesses, individual's clearance levels, and details of future travel can also expose an individual to one or more of the risks discussed above.

c. When deciding whether to notify due to the possibility of identity theft, it is important to consider that an SSN alone can result in identity theft. Additionally, certain combinations of information can have the same effect. A breach involving full name, address, and telephone number when combined with one or more of the following can also result in identity theft: (1) a government-issued identification number (e.g., driver's license number; (2) a biometric record (e.g., fingerprint or eye scan data); (3) a financial account number together with a Personal Identification Number (PIN) or password, if a PIN or password is needed to access the account; (4) health record number; or (5) any information that helps to identify a particular individual (e.g., club membership or customer relationship). If a breach does not involve this type of information, the risk or identity theft is, most likely, minimal, and does not trigger the requirement to notify.

5. Ability to Mitigate. When a breach involves an IT system, the risk of harm will be dependent on the organization's ability to prevent further compromise of the system. In addition to containing the breach, countermeasures such as auditing for signs of misuse of PII and patterns of suspicious behavior should be implemented. While these measures may not prevent the use of PII for identity theft, they may help to limit the harm associated with the breach.

Enclosure H

Sample Notification Letter

Dear John Doe,

I am writing you with important information regarding a breach of your personal information from the U. S. Africa Command that occurred on [ENTER DATE]. The details of the breach are as follows:

What happened? Provide a description of what happened, how the event was discovered, and the date of the discovery.

What information was involved? Provide information about the exact data elements that were exposed (e.g., name, home address, telephone number, and DoD ID number).

What are we doing about it? Include information about how the investigation was conducted, what the findings of the investigation were, and who the attacker was (if known). If a staff member was involved, include a discussion about what measures were taken to correct the situation (training, disciplinary action, etc.). Discuss what measures USAFRICOM is undertaking to try to ensure that similar breaches do not occur in the future.

Are we offering credit monitoring services? If credit monitoring is being provided, provide instructions on how the individual affected may activate credit monitoring.

What can they do? Provide an explanation that the individual affected my wish to consult the FTC Website about data breaches for more information. The FTC Data Breach webpage may be found at: https://www.identitytheft.gov/databreach.