SDDC Pamphlet 340-21

Office Management:

Standard Operating Procedure for the Personally Identifiable Information (PII) Core Management Group (CMG)

Headquarters, Military Surface Deployment and Distribution Command
1 Soldier Way
Scott AFB IL 62225-5006
5 December 2014

UNCLASSIFIED

SUMMARY of CHANGE

SDDC Pam 340-21
Standard Operating Procedure for the Personally Identifiable Information (PII) Core Management Group (CMG)

This is a new issuance.

DEPARTMENT OF THE ARMY
HEADQUARTERS, MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
1 SOLDIER WAY, SCOTT AIR FORCE BASE IL 62225-5006

SDDC PAMPHLET NO. 340-21

5 December 2014

Information Management

STANDARD OPERATING PROCEDURE FOR THE PERSONALLY IDENTIFIABLE INFORMATION (PII) CORE MANAGEMENT GROUP (CMG)

1. Purpose. This standard operating procedure (SOP) provides written guidance, defines responsibilities, and describes procedures for the personally identifiable information (PII) core management group (CMG), Headquarters, Military Surface Deployment and Distribution Command (SDDC).

2. Applicability. This SOP applies to HQ SDDC and subordinate commands assigned to SDDC.

3. Scope. This SOP prescribes official command guidance for an effective response to a breach of PII.

4. Responsibilities. The CMG will manage incidents of a potential or actual PII breach.

a. SDDC Chief of Staff (CofS):

(1) Will convene and chair CMG meetings within 24 hours of notification of a PII breach, as required.

(2) Will maintain CMG alert roster that will reside within the Command Operations Center.

(3) Will immediately notify the SDDC Commander of PII breach within HQ SDDC and/or subordinate units.

b. Deputy Chief of Staff (DCS), G-1, will:

(1) Incorporate PII protection for in/out-processing procedures for civilian and military members.

(2) Maintain and safeguard an accurate record of mailing addresses of current and former employees and service members.

(3) Assist in the timely identification of current and former employees affected by a breach.

(4) Assist designated lead staff in the drafting and mailing of notification letters.

(5) Provide labor/relations advice and guidance.

(6) Participate as a member of the CMG.

c. DCS, G-2, will:

(1) Alert the intelligence community and United States Cyber Command, as applicable, to the potential PII breach to determine foreign involvement immediately upon receipt.

(2) Provide Executive Summary (EXSUM) to SDDC CofS within 24 hours after notification of foreign involvement in a PII breach, and every 24 hours thereafter until final determination/conclusion.

(3) Prepare periodic updates for the CMG on the status of investigations involving foreign entities.

(4) Participate as a member of the CMG and serve as the chief advisor on Foreign Intelligence Service threat and reporting.

(5) Follow-up on initial contact notification for updates, final conclusion and disposition.

(6) Assist and coordinate with the G-6 Privacy Official (PO) to determine type/extent of PII breach.

(7) Coordinate and share with the PO, all information related to investigations of all PII breaches until a determination is made as to whether the incident is foreign or domestic. If foreign, continue to work with PO until final conclusion and disposition.

d. DCS, G-3, will:

(1) When criminality is suspected, immediately notify appropriate Army and civilian law enforcement agencies, the U.S. Army Criminal Investigation Command (USACIDC), DA G-3/5/7, and the USACIDC Computer Crime Investigative Unit.

(2) Report status of criminal investigations.

(3) Participate as a member of the CMG.

e. DCS, G-6, will:

(1) Appoint a PO.

(2) Assess breach as PII or other issue.

(3) Notify SDDC CofS of event.

(4) Advise on a mitigation strategy.

(5) Begin data and fact collection, with Information Assurance assistance as required, to report to CMG and others as needed.

(6) Responsible for all external notifications to HQ AMC and HQ DA.

(7) Report the suspected or actual loss to United States-Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within one hour of discovery.

(a) Notify Army leadership that an initial report has been submitted (usarmy.belvoir.hqda-oaa-aha.bmx.rmda-foia-privacy-alert@mail.mil).

(b) Report the suspected or actual loss to the Army Freedom of Information Act/Privacy Act (FOIA/PA) Office within 24 hours of discovery by completing the DOD PII Incident Reporting Template located at https://www.rmda.army.mil/organization/pa-guidance.shtml. (NOTE: Email the completed template to usarmy.redstone.usamc.mbx.privacy@mail.mil.)

(8) Create and maintain a shared activity summary file folder on the SDDC portal.

(9) Lead PII protection-related training for SDDC to include all required DOD and DA Privacy Act training.

(10) Develop and coordinate minutes of all CMG meetings and post in CMG Community of Practice (CoP).

(11) G-6 will provide an EXSUM to the SDDC CofS summarizing progress within 24 hours of notification of a High Impact PII breach and every 24 hours thereafter until final determination/conclusion.

(12) Participate as a member of the CMG.

f. DCS, G-8, will: When directed by the SDDC CofS, review the budget for impacted unit to determine availability of funds to cover services necessary to reduce or eliminate damage caused by the breach of PII for affected SDDC employees. If the unit does not have funds available, G-8 will identify a funding source and make funds available. If the breach was due to negligence on the part of entities outside SDDC, G-8 will centrally fund the cost.

(1) Funding will cover the cost of providing individual credit monitoring for all affected employees if they desire the service.

(2) Funding will also cover expert identity theft breach analysis to provide information to determine what additional actions will be necessary to protect affected SDDC employees.

(3) Coordinate with the Managers' Internal Control Program representatives in each staff section to ensure the following:

(a) Identify pertinent controls for their areas of responsibility IAW AR 11-2.

(b) Schedule evaluations of controls in their individual management control plans.

(c) Perform evaluations to test controls and document results.

(4) Participate as a member of the CMG.

g. Command Affairs will:

(1) Notify HQ AMC Office of Public and Congressional Affairs of the PII breach.

(2) Advise the SDDC Commander and CofS on messages to the workforce.

(3) Respond to media queries regarding the PII breach.

(4) Respond to Congressional queries regarding the PII breach.

(5) Participate as a member of the CMG.

h. Office of the Staff Judge Advocate will:

(1) Upon request from the PO, review any changes/updates to statutes, Office of Management and Budget (OMB), DOD and DA regulations, directives and policy memorandums involving PII to ensure proper legal interpretation and guidance is available to the CMG.

(2) Advise the command on any potential disciplinary action resulting from a PII breach.

(3) Provide legal advice to the command group, CMG, and PO on PII breach matters, as necessary.

(4) Participate as a member of the CMG.

i. Internal Audit Office will evaluate compliance with requirements contained in this SOP and command policies.

j. Office of the Inspector General will:

(1) Be the commander's eyes and ears regarding implementation and adherence to policies and procedures.

(2) Inspect, investigate, and perform inquiries regarding PII compromise or possible compromise, in accordance with AR 20-1.

(3) Participate as a member of the CMG.

k. The CMG will:

(1) Meet within 24 hours of notification of a potential/actual PII breach.

(2) Meet annually, at a minimum, and as required by the SDDC CofS.

(3) Ensure each principal appoints his/her respective member in writing.

(4) Provide subject matter expert assistance to functional staff counterparts.

(5) Provide and maintain alert roster with on/off-duty contact information for the SDDC CofS.

(6) Maintain and provide updates to the CMG SOP at least annually.

(7) Provide input and post information in the CoP located on the SDDC portal.

l. The PO will:

(1) Provide annual and as required training on protecting PII.

(2) Conduct risk assessment and analysis to determine whether a reported incident is a breach.

(3) Ensure users know how to access and use DD Form 2923, Privacy Act Data Cover Sheet, accessible via http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2923.pdf.

(4) Review holdings of PII annually.

(5) Determine whether the use of a social security number (SSN) is redundant and can be reduced as required by Office of Management and Budget Memorandum M 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

(6) Explore and recommend alternatives for the use of SSNs as a personal identifier for both employees and in programs (i.e., surveys, data calls).

(7) Assign PII categories to electronic and hard copy records.

(8) Establish logging and tracking procedures for high impact electronic PII on portable devices and sign them out at the time of removal from the workplace. This may be as simple as creating a spreadsheet with the date, time, type of PII contained on the device, name of the employee removing it from the workplace, and the date and time when it is returned.

(9) Evaluate all requests to remove copies of PII from the workplace for limited periods for employees and make appropriate recommendations to the approving supervisor.

(10) Coordinate and assist system owners or project managers in conducting Privacy Impact Assessments (PIA) for systems belonging to SDDC.

(11) Upon notification from discoverer, report all actual or suspected PII breaches as outlined in this policy.

(12) Participate and provide administrative and functional oversight of the CMG.

m. Supervisors will:

(1) Ensure their employees are adequately instructed in their responsibilities related to PII.

(2) Review all requests to remove copies of PII from the workplace for employees following PO review and recommendation.

(3) Assess the need for collecting PII seeking to minimize or eliminate its use wherever feasible in business processes and documentation.

(4) Ensure compromised PII is reported to the SDDC PO as soon as the breach or suspected breach is discovered.

(5) Ensure employees authorized to telework protect all controlled unclassified information (CUI) as defined in DOD Instruction 5200.01, DOD Information Security Program and Protection of Sensitive Compartmented Information and DOD Instruction 1035.01, Telework Policy.

n. SDDC military, civilian, and contractor personnel will:

(1) Complete annual and as required Privacy Act training.

(2) Immediately report compromised PII to their supervisor and the SDDC PO.

(3) When transmitting PII via email or any other electronic means, encrypt and digitally sign messages. Only distribute PII to those with a bona fide need for the information.

(4) Submit written requests to remove copies of PII from the workplace for limited periods to their supervisor for review and PO recommendation.

(5) Treat Privacy Act data as "For Official Use Only" (FOUO).

(a) Should an SDDC employee have a bona fide need to collect and use PII, they must protect the PII file from accidental disclosure to unauthorized parties. All personnel are responsible for protecting PII information.

1. PII is considered and must be afforded the protection extended to FOUO.

2. PII is considered information that, if wrongfully released, could reasonably be expected to constitute an unwarranted invasion of the personal privacy of an individual.

3. As such, PII is exempt from mandatory disclosure under the Freedom of Information Act (FOIA), exemption 6.

(b) Adhere to special handling for files containing PII. Employees who need to handle PII need to take precautions in the handling and storage of files containing PII. The following rules apply to all files containing PII regardless of the medium.

1. Access to FOUO: Files containing PII are FOUO. FOUO information may be disseminated within DOD components, between officials of those components or DOD contractors, consultants, and grantees as necessary during official duty.

2. Government Branches: FOUO information may be disseminated to the Executive and Judicial Branches in performance of a valid government function.

3. Congressional Inquiries: FOUO files containing PII may be disclosed to Congress only in accordance with DOD Instruction 5400.04, Provision of Information to Congress.

4. Question Access Rights: Never assume someone has a valid need-to-know. Ask questions to establish a bona fide need-to-know.

5. Verify Access: Verify that only those given explicit permission to access a file containing PII can do so. Never share or discuss information with unauthorized individuals.

6. Assess Risk: Supervisors or individuals will determine the risk level of each identified file using the five factors identified in the risk assessment model (Appendix C) that should be considered to assess the likely risk of harm.

(c) Digital Files: When creating a digital file, such as a Word document, Excel spreadsheet, or Access database, the file owner must ensure it is properly protected.

1. Ensure approved data-at-rest (DAR) encryption tools are used on any desktop or mobile device that contains sensitive information, such as PII. Only government furnished devices may be used. Individuals will ensure they use these tools to protect PII content.

2. If placing a file containing PII in a multi-user accessible location such as a network drive or Army Knowledge Online (AKO) team site, the file owner must verify who has a need to know and explicitly grant those users file rights, while implicitly denying access to everyone else using role-based security.

3. Material containing PII must bear markings that alert the holder or viewer that the material contains FOUO information (i.e., FOUO or PA) in the title of the electronic file.

4. Encryption: Digital files containing PII must be encrypted when not in use. When sent via email, they must also be encrypted every time.

5. Email: Any email message containing PII must be encrypted and labeled “For Official Use Only” (FOUO).

6. Email with PII Attachment: An email containing a PII attachment (such as a Word document) must be labeled “FOUO” Attachment, or language to that effect.

7. Transmission Outside DOD: Digital files containing PII must bear an expanded marking when being transmitted outside the DOD. A statement similar to this one should be used: "This document contains information exempt from mandatory disclosure under FOIA--Exemption 6 applies."

8. Labeling: Digital files containing PII must be labeled as “FOUO” on the top and bottom of every page, or at some other appropriately noticeable section (such as the top row of a spreadsheet or in the description of a database table).

9. Removable Media: Individuals are personally responsible and must maintain accountability for government-owned mobile computing devices and data storage devices. Individuals must ensure PII is protected with an approved DAR encryption tool and physically secure the media at all times. Do not leave media unattended.

10. Shared Network Storage: PII may not be stored on shared drives unless proper access controls are in place to prevent unauthorized viewing. This means that people allowed to view the file must be explicitly identified while all others are implicitly denied.

11. Public Folders: Files containing PII must never be posted on Intranet/Internet web sites or public folders without explicit supervisor approval and proper access controls.

(d) Hard copy Files: When creating a hard copy file containing PII, the file owner must take reasonable precautions to ensure that only those with a need-to-know will view the file.

1. Markings: Writers must ensure that PII containing hard copies are properly marked at time of printing. The file should be labeled UNCLASSIFIED/FOR OFFICIAL USE ONLY. This label should be on the bottom of the front cover (if there is one), the title page (if there is one), the first page and the outside of the back cover (if there is one).

2. Cover Sheet: Obtain a copy of DD Form 2923, Privacy Act Data Cover Sheet, to help ensure proper markings and protect from prying eyes. Cover sheets can be found at: http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2923.pdf.

3. Document Duplication Awareness: Writers must be aware if they copy documents that they ensure sensitive data is not duplicated in the new document (i.e., word tracking/notes pages/comments).

4. Storage During Work: Reasonable steps must be taken during duty hours to store PII. This means keeping information off the desk when not in use and out of general sight when in use.

5. Storage After Work: After working hours, files containing PII must be stored in a secure manner. If being stored within a government or government-contracted building with security, information may be stored in unlocked containers, desks or cabinets. If otherwise, then use locked desks, file cabinets, bookcases, locked rooms, or similar items.

6. Mailing PII: Files containing PII must be transmitted via first-class mail or parcel post. If the shipment of PII files is bulk, then fourth-class mail may be used.

7. Facsimile Transmission: If sending a facsimile of a file containing PII, approved secure communications systems should be used. Additionally, a facsimile transmission must use a cover sheet, DD Form 2923.

(e) Destruction of Files Containing PII: Files containing PII fall under several larger categories, from official Army correspondence to payroll information. Each category of information has its own mandatory retention period.

1. Army Records Information Management System (ARIMS): Use ARIMS to determine how long you must keep a file containing PII. This retention time will most likely not be determined by the fact that the file contains PII (unless the file is an official document created under FOIA or the Privacy Act). If needed, seek assistance from the SDDC Records Manager.

2. Digital Files: Digital files containing PII should be destroyed in whatever way renders them least likely to be recovered. The details of how to do this varies from system to system, but below are a few examples.

a. Local Computer/Network Folder: To destroy a file off a network file share or local computer folder, press Shift + Delete.

b. Outlook Email: To destroy an email in Microsoft Outlook, select the file and press Shift + Delete.

c. Removable Media: To destroy removable media, such as compact discs or decommissioned drives, use a GSA-approved shredder or contact the PO who can assist.

d. Hard copy Files: Hard copy files containing PII should be shredded when ready for destruction using an approved shredder.

5. Breach Reporting. In the event of a breach:

a. Immediately following a violation, the individual or organization discovering the actual or suspected breach/compromise of PII will report the incident to his or her supervisor and the PO. The staff section of SDDC CIO will report the potential/actual incident to the SDDC CofS. A General Breach Process Checklist/Questionnaire is located at Appendix B. This checklist is used to document and report the PII Breach.

(1) Within 1 Hour: The PO shall notify the staff section of the SDDC CIO of a potential breach in order to assess and evaluate the incident and determine if a suspected or actual breach occurred. Once the determination has been made that a breach occurred, the PO will report the incident to US-CERT at http://www.us-cert.gov within 1 hour of a verified breach. Immediately following the US-CERT notification, the PO will send an email reporting the incident to usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil as notification to Army Privacy Office leadership to inform them of the initial report to US-CERT.

(2) Within 24 Hours: The PO will report all incidents involving actual or suspected breach/compromise of PII to the Army Freedom of Information Act/Privacy Act (FOIA/PA) Office within 24 hours of discovery by completing the DOD PII Incident Reporting Template located at https://www.rmda.army.mil/organization/pa-guidance.shtml and emailing the completed template to usarmy.redstone.usamc.mbx.privacy@mail.mil, subject: PII Breach Reporting. As additional information is gathered, updates should be made to the template and resubmitted to the Army Privacy Office. The SDDC PO (or a designee) will be courtesy copied on all correspondence.

b. The SDDC Command Operations Center (COC) will notify the SDDC PO immediately upon receipt of the initial Commander's Critical Information Requirement (CCIR) report from an SDDC brigade or battalion. After assessing the incident, the SDDC PO will notify the SDDC CofS. The SDDC CofS may convene a meeting of the Core Management Group (CMG) after notification of a breach to assess the level of risk caused by the breach and develop a command

action plan. The CMG will include senior level personnel from the following staff elements: DCS, G-1/4; DCS, G-2; DCS, G-3; DCS, G-6; DCS, G-8; Command Affairs; Staff Judge Advocate; and the Inspector General.

c. In the event of a breach an assessment shall be made to determine whether notification of a breach is required. The assessment will consider the likelihood of the risk to the individual and of the harm caused by the breached information.

(1) The CMG or CIO/G-6 will assess the likely risk of harm using appendix C. SDDC will consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved.

(2) SDDC will bear in mind that notification when there is little or no risk of harm might create unnecessary concern and confusion.

(3) SDDC will document its rationale and the resulting "risk level" for not providing a notification if the risk assessment determines notification is not required. If a notification is not necessary, the SDDC PO will draft a memorandum and submit it to the HQ AMC Privacy Office for further distribution to the Army Privacy Office.

(4) When personal information is maintained by a contractor on behalf of SDDC, the contractor shall notify the SDDC PO, through proper contracting channels to include the Contracting Officer Representative immediately upon discovery that a loss, theft, or compromise has occurred.

(a) The CMG shall determine whether the government or contractor shall make the required notification in accordance with contract terms.

(b) If the contractor is to notify the impacted population, the contractor shall submit the notification letters to the CMG for review and approval. The CMG shall coordinate with the contractor to ensure the letters meet the requirements of this policy.

(c) If it is determined that notification is necessary and appropriate, SDDC leadership, in coordination with the CMG, will determine whether any protective services, such as credit monitoring, will be provided to the affected individuals. The SDDC DCS, Resource Management (G-8), will provide necessary funding to cover services necessary to reduce or eliminate damage caused by breach of PII by any SDDC procedure or action with proper authorization.

(5) Internal Notifications:

(a) The SDDC DCS, G-3 Protection Division will make all notifications to any military intelligence agency in the event a foreign entity and/or classified information are involved in the PII breach.

(b) The SDDC DCS, G-3 Protection Division will lead any additional reporting to Army and civilian law enforcement agencies.

(c) If the incident involves government credit card data, the PO or designee, will notify the issuing bank.

(6) External Notifications:

(a) The SDDC Commander, director or designee will notify all affected individuals when identified of an incident as soon as possible, but no later than 10 days after the breach is discovered.

(b) In some circumstances, law enforcement or national security considerations may require a delay if notification would seriously impede the investigation of the breach or when notification could increase a risk of harm to the affected individuals.

(c) Decisions to delay notification must be approved by SDDC CofS. If it is determined that notification should be delayed, SDDC will submit a memorandum through the chain of command to the Department of Army Senior Agency Official for Privacy who will forward it to the Defense Privacy Office. Any delay should not exacerbate risk or harm to any affected individual(s).

(d) Notification to affected individuals will be made in writing via U.S. Postal Service first-class mail, email, or hand delivery and at a minimum will include: 1) a brief description of what happened; 2) date(s) of occurrence and discovery; 3) a description of types of personal information involved; 4) a statement of whether information was encrypted or protected by other means; 5) steps individuals should take to protect themselves from potential harm; and, 6) what the command is doing to investigate the breach to mitigate losses and to protect against further breaches. All notification information will comply with the guidance in DOD 5400.11-R, paragraph C1.5.

(e) First-class mail with a return-receipt confirmation will be the primary means of notification. Email notification will only be used if affected individuals have provided an email address and expressly consented to email as the primary means of communication with the command.

(f) SDDC PO will solicit positive confirmation from affected individuals that they have been notified. A report will be provided to the SDDC CofS and appropriate commander/director of those who have been notified.

(g) A generalized (substitute) notice should be given to potentially affected individuals by whatever means is most likely to reach the affected individuals if SDDC cannot readily identify the affected individuals or will not be able to reach the individuals.

(h) The SDDC PO will work with SDDC Command Affairs to determine if a public announcement on the breach should be made. The CMG will recommend determination to release the public announcement.

1. Individual notification may be supplemented by placing notifications in newspapers, broadcasts, and other public media outlets (i.e., web site) or third parties that will reach the affected individuals.

2. The notifications will be carefully planned and provide information to handle inquiries from the affected individuals and the public.

3. Media notification shall be promptly prepared for approval by the CMG when the breach is significant (e.g., the PII is highly sensitive) and the risks and potential for harm to the individuals involved as a result of the breach are greater than the risks and potential for harm to the investigation as a result of public disclosure of the breach. The actions taken to inform the media are necessary to preserve the public's trust.

4. CofS will designate a CMG member to conduct an after action review of the incident and handling of the breach after the incident.

The proponent of this regulation is the Chief Information Officer/G-6, Military Surface Deployment and Distribution Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to HQ SDDC, Attn: AMSSD-IMO-B, 1 Soldier Way, Scott AFB IL 62225-5006.

SUSAN A. DAVIDSON
Major General, USA
Commanding

APPENDIX A
References

Section I
Required Publications

Office of Management and Budget Memorandum M-07-16
Safeguarding Against and Responding to the Breach of Personally Identifiable Information

DODM 5200.01, Volume 1
DOD Information Security Program: Overview, Classification, and Declassification

DODD 5400.11
DOD Privacy Program

DOD 5400.11-R
Department of Defense Privacy Program

AR 25-2
Information Assurance

AR 340-21
The Army Privacy Program

AMC Pamphlet 25-51
Standard Operating Procedures (SOP) for the Personally Identifiable Information (PII) Core Management Group (CMG)

AMC CPM 25-114
Command Policy Memorandum – Protecting Personally Identifiable Information (PII) and PII Breach Notification Policy

Section II
Related Publications
A related publication is merely a source of additional information.

This section contains no entries.

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

DA Label 87
For Official Use Only

DD Form 2923
Privacy Act Data Cover Sheet

DD Form 2930
Privacy Impact Assessment (PIA)

DD Form 2959
Breach of Personally Identifiable Information (PII) Report

APPENDIX B
General Breach Process Checklist/Questionnaire

SDDC Breach Incident Checklist			
Thoroughness is more important than speed			
Incident Date:			
Reported by (Directorate/Brigade):			
Was the incident:	☐Suspected	☐Confirmed	
Type of incident:	☐Paper	☐Electronic	
	☐Theft	☐Lost	☐Unauthorized Access
Safeguards:	☐Encryption/DAR	☐CAC Enabled	
Describe how breach happened:			
Containment Occur? Date_____ Time: _____ How was it contained?			
Steps to prevent recurrence/mitigation?			

Step Number	Process Step/Question	Responses		Completed/ Comments
		Yes	No	
Initial Discovery of a Breach Incident (lost, exposed, or network compromise)				
1.	If incident involves a lost electronic device, report the missing device to local law enforcement (obtain a report).			
2.	Report incident to supervisor and local privacy official.			
3.	If incident involves a missing computing device (e.g., laptop, personal electronic device), notify security official(s).			
4.	Report breach incident to SDDC Privacy Office, RMDA (email: usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil) and US-CERT (http://www.us-cert.gov) within 1 hour of suspecting a breach occurred.			
5.	Notify Army Freedom of Information Act (FOIA/PA) Office (https://www.rmda.army.mil/index.html) and HQ AMC Privacy Office (usarmy.redstone.usamc.mbx.privacy@mail.mil) within 24 hours.			
Privacy Official Receiving Notification				
6.	Did the original incident occur with an SDDC employee or did SDDC employee extend breach (e.g., forward an email with sensitive data)?			
7.	Did the incident occur with a contractor? Did the contractor notify SDDC immediately? Core Management Group (CMG) will determine whether contractor will make required notification (letters will be submitted to CMG for review prior to sending).			
8.	What PII was potentially breached? ☐Name ☐SSN ☐DoB ☐Phone number/address ☐Financial ☐Medical ☐Other Determine what was exactly compromised and who was affected. Do not want to notify and cause stress for people that were not affected).			
9.	Did the individual(s) that now have the information have a need-to-know?			
10.	Safeguards to protect the information (e.g., data at rest, CAC, masking of PII) were verified by network?			
11.	SDDC G-3, Protection Division, will make all notifications to any military intelligence agency in the event a foreign entity and/or classified information are involved in the PII breach POC at intelligence agency.			
12.	If the incident involves government credit card data, has the issuing bank been notified?			
13.	Complete a CCIR (Trigger #7), if required.			
14.	All commanders, staff principals, and directors will notify the SDDC CMG, through the SDDC Command Operations Center.			

Step Number	Process Step/Question	Responses		Completed/ Comments
		Yes	No	
15.	The SDDC Chief of Staff will call a meeting of the CMG after notification of a breach to assess the level of risk caused by the breach and develop a command action plan. The CMG will include senior level personnel from the following staff elements: ☐ Deputy Chief of Staff, G-1/4 Name: ☐ Deputy Chief of Staff, G-2 Name: ☐ Deputy Chief of Staff, G-3 Name: ☐ Deputy Chief of Staff, G-5 Name: ☐ Deputy Chief of Staff, G-6 Name: ☐ Deputy Chief of Staff, G-8 Name: ☐ Command Affairs Name: ☐ Staff Judge Advocate Name: ☐ Inspector General Name:			
16.	The CIO/G-6 will assess the likely risk of harm based on the Risk Assessment Model. (CMG will consider a wide range of harms, such as harm to reputation for harassment or prejudice, particularly when health of financial benefits information is involved in the breach. CMG will keep in mind that notification when there is little or no risk of harm might create unnecessary concern or confusion.)			
17.	Actions take to minimize exposure: ☐Law Enforcement ☐Media ☐Web site taken down ☐Offer credit monitoring (not offering could lead to negative press) ☐Notify individuals ☐Other:			
18.	If required, SDDC CofS or designee will notify all affected individuals identified in their command's incident as soon as possible, but no later than 10 days after the breach is discovered and the identities of individuals possibly compromised are ascertained. (In some circumstances, law enforcement or national security considerations may require a delay if notification would seriously impede the investigation of the breach or when notification could increase a risk of harm to the affected individuals.)			

Step Number	Process Step/Question	Responses		Completed/ Comments
		Yes	No	
19.	If it is determined that notification should be delayed, SDDC will submit a memorandum through HQ AMC Privacy Office to the Senior Army Official for Privacy who shall forward it to the Defense Privacy Office.			
20.	Determine disciplinary actions are to be taken. (Did the individual have permissions to transport lost data? Were safeguards in place at the time of the incident?)			
21.	Should Command Affairs make a statement?			
22.	Was credit monitoring provided? When directed by the SDDC CofS, G-8 will provide necessary funding to cover credit monitoring services as deemed necessary to reduce or eliminate damage caused by breach of PII due to an SDDC procedure or or action.			
23.	Was a call center established? Call center should be manned by qualified Command Affairs staff versed in what to say and how to handle upset individuals.			
24.	Was notification sent to affected individuals within 10 days of the incident?			
25.	Were records kept for a specified and approved time? All correspondence will be maintained. Actions taken to track individuals that could not be notified will be recorded should individuals request information at a later date.			
26.	Was an after action review conducted? Review procedures and update as necessary.			

APPENDIX C
Identity Theft Risk Analysis

1. Five factors to consider when assessing the likelihood of risk and/or harm:

a. Nature of the data elements breached.

(1) The nature of the data elements comprised is a key factor to consider in determining when and how notification should be provided to affected individuals. For example, theft of a database containing an individuals' name in conjunction with SSNs, and/or dates of birth may pose a high level or risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.

(2) 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 is contextual. A name in one context may be less sensitive than in another context. In assessing the levels of risk and 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.

b. 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 only determining factor for whether an agency should provide notification.

c. Likelihood the information is accessible and usable.

(1) Upon learning of a breach, agencies 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.

(2) Depending upon the number of physical, technological, and procedural safeguards employed by the agency, the fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. If the information is properly protected by encryption, for example, the risk of compromised may be low to nonexistent. In this context, proper protection means encryption has been validated by National Institute of Standards and Technology.

(3) Agencies will first need to assess whether the breach involving PII is at a low, moderate, or high risk of being used by unauthorized persons to cause harm to an individual or group of individuals. The assessment should be guided by NIST security standards and guidance. Other considerations may include the likelihood an unauthorized individual will know the value of the information and either use or sell the information to others.

d. Likelihood the breach may lead to harm.

(1) 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." Additionally, agencies should consider a number of possible harms associated with the loss or compromised of information. Such harms may include the effect of a breach of confidentiality or fiduciary

responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

(2) The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. SSNs and account information are useful to committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other PII, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients patients at a clinic for treatment of a contagious disease.

(3) In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance for the Identity Theft Task Force found at www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

e. Ability of the agency to mitigate the risk of harm. Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others may, particularly where the potential injury is more individualized and may be difficult to determine.

2. SDDC will thoroughly document the circumstances of all breaches of PII and the decisions made relative to the factors above in reaching their decision to notify or not notify individuals.

RISK ASSESSMENT MODEL

No.	Factor	Risk Determination: Low Moderate High	Comments: All breaches of PII, whether actual or suspected, require notification to US-CERT. Low and Moderate risk/harm determinations and the decision whether notification of individuals is made rest with the head of the DOD component where the breach occurred. All determinations of high risk should result in activation of the CMG.
1	What is the nature of the data elements breached? What PII was involved?		
	a. Name only	Low	Consideration needs to be given to unique names, those where one or only a few in the population name have or those that could readily identify an individual, i.e., public figure
	b. Name plus one or more personal identifier (not SSN, medical or financial)	Moderate	Additional identifiers include date and place of birth, mother's maiden name, biometric record and any other information that can be linked or is linkable to an individual
	c. SSN	High	
	d. Name plus SSN	High	
	e. Name plus medical or financial data	High	
2.	Number of individuals affected		The number of individuals involved is a determining factor in how notifications are made, not whether they are made*

No.	Factor	Risk Determination: Low Moderate High	Comments: All breaches of PII, whether actual or suspected, require notification to US-CERT. Low and Moderate risk/harm determinations and the decision whether notification of individuals is made rest with the head of the DOD component where the breach occurred. All determinations of high risk should result in activation of the CMG.
3.	What is the likelihood the information is accessible and usable? What level of protection applied to this information?		
	a. Encryption (FIPS 140-2)	Low	
	b. Password	Moderate/High	Moderate/High determined in relationship to category of data in No. 1
	c. None	High	
4.	Likelihood the breach may lead to harm	High/Moderate/ Low	Determining likelihood depends on the manner of the breach and the type(s) of data involved
5.	Ability of the agency to mitigate the risk of harm		
	a. Loss	High	Evidence exists that PII has been lost; no longer under DOD control
	b. Theft	High	
	c. Compromise		
	(1) Compromise within DOD control	Low High	No evidence of malicious intent. Evidence or possibility of malicious intent
	(2) Compromise beyond DOD control	High	Possibility that PII could be used with malicious intent or commit ID theft

*High Impact. Any Defense-wide organizational (e.g., unit or office) or program or project level compilation of electronic records containing PII on 500 or more individuals stored on a single device or accessible through a single application or service, whether or not the compilation is subject to the Privacy Act. Also, any compilation of electronic records containing PII on less than 500 individuals identified by the Information or Data Owner as requiring additional protection measures. Examples: A single mobile computing or storage device containing PII on 500 or more individuals, even if the PII is distributed across multiple files or directories, is considered High Impact PII. A DOD

enclave of 500 or more users, with the PII for each user embedded in his/her individual workstation, is not considered High Impact PII.

Moderate Impact. Any electronic records containing PII not identified as High Impact, reference 1e.

Glossary

Section I
Abbreviations

AKO
Army Knowledge Online

ARIMS
Army Records Information Management System

CIO
Chief Information Officer

CMG
core management group

COC
Command Operations Center

CoP
community of practice

CofS
Chief of Staff

DAR
data-at-rest

DCS
Deputy Chief of Staff

DOD
Department of Defense

EXSUM
executive summary

FOIA
Freedom of Information Act

FOUO
for official use only

OMB
Office of Management and Budget

PA
Privacy Act

PIA
privacy impact assessment

PII
personally identifiable information

PO
privacy officer

SDDC
U.S. Army Military Surface Deployment and Distribution Command

SOP
standard operating procedure

USACIDC
U.S. Army Criminal Investigation Command

US-CERT
United States-Computer Emergency Readiness Team

Section II
Terms

This section contains no entries.

Section III
Special Abbreviations and Terms

This section contains no entries.