USAR Regulation 25-5

Information Management: Records Management

Protecting and Reporting Compromised Personally Identifiable Information (PII)

Department of the Army
Office of the Chief, Army Reserve
Washington, DC 20310-2400
1 December 2010

SUMMARY OF CHANGE

USAR Regulation 25-5, Protecting and Reporting Compromised Personally Identifiable Information (PII)

This regulation, dated 1 December 2010--

- Delineates command policy on the protection of records containing personally identifying information related to Army Reserve Soldiers, DAC employees and/or any other category of personnel in association with the Army Reserve.

- Specifies PII breach reporting requirement websites and email addresses (para B-3b).

- Prescribes USAR Form 160-R, Personally Identifiable Information (PII) Breach Report (para B-3b(3))

DEPARTMENT OF THE ARMY
Office of the Chief, Army Reserve
Washington DC 20310-2400
1 December 2010

USAR Regulation 25-5

Information Management: Records Management

Protecting and Reporting Compromised Personally Identifiable Information (PII)

For the Commander:

WILLIAM J. GOTHARD
Brigadier General, United States Army
Chief of Staff

Official:

John P. Donovan
JOHN P. DONOVAN
Colonel, GS
Deputy Chief of Staff, G-1

History. This is a new USAR regulation.

Summary. This regulation prescribes policies, procedures, and responsibilities for the protection of PII for all Army Reserve personnel (military, DAC, contractors, etc.)

Applicability. This regulation applies to all uniformed members of the Army Reserve, and to its civilian workforce, both Federal and contracted.

Proponent and exception authority. The Deputy Chief of Staff, G-1 is the proponent for this regulation. The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The proponent may delegate this approval authority, in writing, to a division or branch chief under their supervision within the proponent agency, in the grade of colonel or civilian equivalent.

Army Management Control Process. This regulation does not contain management control provisions.

Supplementation. Supplementation of this regulation and the establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G-1 (ARRC-PRA-R), 1401 Deshler St. SW, Fort McPherson, GA 30330-2000.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, USARC, ATTN: ARRC-PRA-R, Fort McPherson, GA 30330-2000.

Distribution. This publication is available in electronic media on the USARC Intranet website at https://usarcintra/ and on the Army Reserve Component portion of the Army Knowledge Online (AKO) website (http://www.us.army.mil/). This regulation is intended for command level A. Local reproduction is authorized.

Contents (Listed by paragraph number)

Appendixes

Glossary

1. Purpose

This regulation establishes responsibilities at all levels of command in the Army Reserve for the recognition and protection of records containing PII. Specific in-depth guidance for the operation, management, and reporting incidents of PII loss or compromise is also addressed in Appendix B.

2. References

Required and related publications and prescribed and referenced forms are listed in Appendix A.

3. Explanations of abbreviations and terms

Abbreviations and terms used in this publication are explained in the Glossary.

4. Responsibilities

a. Army Reserve commanders at all levels of command and military and civilian supervisors throughout the Army Reserve will ensure that all personnel in their jurisdiction are fully aware of their responsibility to protect Army records containing PII, whether recorded on hard copy or electronic medium. Additionally, in the event PII is compromised, personnel having its custody will fully comply with the reporting procedures established by Department of Homeland Security, Department of the Army (DA) and this Headquarters (see Appendix B). The following staff agencies will form a Response Team in the event of a **serious** PII incident. They are:

(1) The G-1- lead agent in determining if PII has been lost and or compromised and will ensure that all reporting requirements have been met.

(2) The G-3/5/7 - the conduit for all PII incident reporting, providing a 24/7 point of access (AROC), tracking all internal and external suspense dates, and collecting a historical record of all correspondence.

(3) The G-2/6 - responsible for providing and maintaining the automated infrastructure and tools to securely store and transmit all PII for the Army Reserve.

(4) The Army Reserve Communications (ARC/PAO) - will assess the incident and its impact on the command and staff, as well as the potential for command and public information activity.

(5) The Staff Judge Advocate (SJA) - will provide legal guidance and advice concerning all PII incidents and assist in all phases of reporting/follow-on actions. Additionally, the SJA will ensure that the legal review of Army Reserve procurement actions addresses whether the contracts contain necessary PII protection clauses in the statement of work.

b. All USARC/OCAR staff elements are responsible for identifying PII and protecting it appropriately. In the event PII has been lost/compromised, reporting must be immediate and performed as outlined in Appendix B.

c. All subordinate commands will take appropriate measures to safeguard all PII recorded data, regardless of the medium, pertaining to members of their command and their families. The reporting requirements established by DA and this regulation, when PII data is lost or compromised, will be adhered to.

5. Identifying PII

a. Personally Identifiable Information (PII) is prevalent throughout the Army Reserve and many Soldiers, DA civilian personnel and contractors, process this information daily. It is extremely important to identify PII data and protect it from unauthorized disclosure. The cause of PII being compromised, in most instances, begin with the information being misclassified and therefore, not protected properly. The following list/categories, although not exclusive, contains the most obvious types of PII:

(1) Name
(2) Social Security Number (SSN)
(3) Date and place of birth
(4) Mother’s maiden name
(5) Biometric records
(6) Education records
(7) Financial records
(8) Medical records
(9) Criminal records
(10) Employment history

b. In order to be classified as a PII record, the categories listed above must be associated with an individual Soldier, his/her family, DA civilian or contractor. <u>A list of dates and place of birth without individual names would not be considered PII</u>. If in doubt about a particular type of information, contact the headquarters Freedom of Information Act (FOIA) specialists, or the SJA office, for a determination.

6. Protecting PII

Whether PII is in hard copy or in electrons, it is not to be released to anyone who does not have a duty-related official need to know.

a. Hard copies are to be maintained within a facility that controls access and lock-and-key within work areas. Mailing hard copy PII will be by certified return receipt to confirm delivery.

b. Electronic format (electrons) can be classified into two types:

(1) Electronic data in transmission - is information being transmitted from one source to another; for example, email and accessing a web or database application. Data in transmission is to be conducted only by approved encryption standards to maintain confidentiality of the data. While the G-2/6 ensures encryption standards are met for web and database applications, it is the responsibility of every user to encrypt all email that contains PII.

(2) Electronic data at rest - is the physical location of the data when not in transmission, whether on a CD, computer or server. Data at rest is further broken down as static devices and mobile devices.

(a) Static devices are defined as equipment that is not intended to leave the facility, such as workstations and servers. These devices protect PII through user identification controls, and as they are not to leave the secured facility, they are not prone to loss or theft.

(b) Mobile devices are equipment that, by their intended purpose, may leave the facility. Laptops and blackberries fall into this category, as well as diskettes, CD/DVDs and external hard drives. Army policy mandates that all mobile devices must have data at rest encryption enforced. <u>However, since the Army has not approved a data-at-rest solution for CD/DVDs or external hard drives, these devices containing PII will NOT be allowed off an Army Reserve facility</u>. If it is operationally necessary to remove such media from an Army Reserve facility, contact the Chief, Information Assurance Division at (678) 364-8246), USARC G-2/6, for assistance. **Safeguarding PII is the responsibility of the individual user of a mobile device in his/her custody.**

7. Reporting a suspected or confirmed loss

All Army Reserve personnel must report a PII loss immediately to their chain of command, ATTN: PII Specialist, who will contact the command Emergency Operations Center (EOC) and the EOC will then contact the Army Reserve Operations Center (AROC) at (404) 464-8371/8372. The individual having firsthand knowledge of the loss is responsible for submitting the reports described in para B-3b.

Appendix A
References

Army Regulations and DA Forms are available online from the Army Publishing Directorate (APD) website (http://www.apd.army.mil).

Section I
Required publications

This section contains no entries.

Section II
Related publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

USAR Pam 25-2
Information Management: Army Reserve Records Management and Publishing Program (Chapter 4, Handling, Safeguarding and Releasing Official Army Reserve Records)

AR 25-55
The Department of the Army Freedom of Information Act Program (para 1.300, Public Information).

AR 190-40
Serious Incident Report

AR 340-21
The Army Privacy Program

Memorandum
20 Sep 06, Executive Office of the President, Office of Management and Budget, subject: Recommendation for Identity Theft Related Data Breach Notification

Memorandum
18 Aug 06, Department of Defense, subject: Department of Defense (DOD) Guidance on Protecting Personally Identifiable Information (PII)

Message
Army Vice Chief of Staff Army, DTG: 021843Z Jul 07, Subject: Army Protection of Personally Identifiable Information (PII) Awareness

Section III
Prescribed Forms

The following form(s) are available on the USAR Intranet website at https://usarcintra/pubs-forms/pubsform/formindex.html and the Army Reserve Component portion of the Army Knowledge Online (AKO) website (http://www.us.army.mil/).

USAR Form 160-R
Personally Identifiable Information (PII) Breach Report. (cited in para B-3b(3))

Section IV
Referenced Forms

This section contains no entries.

Appendix B
PII Breach Prevention and Reporting

B-1. Personally Identifiable Information (PII) defined

a. Personally identifiable information is any combination of information elements that:

(1) Identify a specific person.

(2) Provides at least one additional element of information pertaining to that person, .i.e., information identified to a specific person. For example, a social security number by itself is not PII; but when combined with the name, home address, or phone number of the person or data subject, then the combination constitutes PII.

b. The PII is one of 9 categories of *For Official Use Only* (FOUO) information. It is information exempt from mandatory disclosure if requested under the provisions of the FOIA. Access to FOUO information is limited to those with a need to know in order to perform their officially assigned duties. The detailed protective measures for PII are the same as for any kind of FOUO information and apply regardless of the medium whether voice, sound recording, paper, or electronic.

B-2. PII breach prevention

a. As all FOUO information, PII must never be left open to view when removed from a container. A DA Label 87, *For Official Use Only*, protective cover sheet, must be placed over any document containing FOUO information, to include PII. Similar cover sheets, *Personal in Nature*, for example, are permissible, but limited to PII.

b. The PII must never be left over night in a motor vehicle or unlocked in a nonfederal building. When not in use, keep it in a closed container, preferably under lock and key, even in a secure building.

c. Documents containing PII are never to be discarded without shredding.

d. Envelopes used to mail documents containing PII must be non show-through; that is, not allow the contents to read through the envelope.

e. Requests for records or information from records should be referred to the FOIA specialists.

f. Emails containing PII should have **FOUO** at the start of the subject.

g. Before faxing PII, phone ahead to alert the intended recipient to be sure he/she are at work and know to check the receiver.

h. Fax machines that print a confirmation of successful transmission which reproduce a portion of the document sent should never be left without taking the confirmation.

i. When printers that were disabled come on line, they will often print documents from the queue. When this occurs, users will periodically check the printer to see whether the documents were printed.

j. PII can be transmitted over a DOD-approved network, such as the USARC Intranet, but never over the Internet or a privately operated system, i.e., gmail, Yahoo, Hotmail, etc.

k. Avoid transmitting PII over voice or data transmission lines that include radio links without scrambling or encryption. If unavoidable, calls should be phrased to get the message across without specifying the PII.

l. Delete home phone numbers from cellular phones and similar devices that record this information.

m. Portable devices and media without Army-approved encryption software must never be allowed to download PII.

n. Portable devices and media that store PII must have Army-approved encryption software, reduce the number of records to the absolute minimum necessary, and be kept out of sight and under lock and key at all times.

o. When proposed or due for renewal, any contract allowing contractor personnel access to or custody of PII must be coordinated with headquarters privacy specialists.

p. Do not transmit PII to a commercial backup, printing, address labeling, or mailing service.

q. No printer, fax machine, or copier will be turned in/disposed of without making certain that the internal hard drive has been erased/removed.

B-3. PII breach serious incident reporting

a. Breach reporting consists of submitting serious incident reports to the US-Computer Emergency Response Team (US-CERT)/Department of Homeland Security (DHS), the AROC, DA, and notifying the individuals whose PII may be compromised. The reports must be as open, accurate, and thorough as possible. The alert to the field must include guidance to mitigate any consequences that could result from the breach.

b. PII breach will - (see flow chart at Appendix C)

(1) **Immediately** be reported, by the individual/individuals closest to the incident, to his/her chain of command. The command's emergency operations center will relay the information to the AROC at (404) 464-8371/8372 (email at usarcaroc@usar.army.mil) and the AROC will notify the Chief of Staff.

(2) **Within the first hour** of discovery, go to the US-CERT website at http://www.us-cert.gov/, (see "Reporting" left-hand side and select Report an Incident) and email pii.reporting@us.army.mil to notify Army leadership of the initial report to US-CERT.

(3) **Within 12 hours** of discovery, fill out USAR Form 160-R, Personally Identifiable Information (PII) Breach Report (see sample at figure B-1) and submit to the USARC G-1, Privacy Specialist(s) at david.s.goldsmith@usar.army.mil / hector.morales1@usar.army.mil.

(4) **Within 24 hours** of discovery, notify the Records Management and Declassification Agency (RMDA) at https://www.rmda.army.mil/privacy/foia-incidentreport1.asp and filling out the Army's privacy incident report. *Note: If the website is unavailable, contact the USARC Privacy Specialist(s) (see email addresses above), who will contact RMDA.*

c. The PII specialist at the major subordinate commands (MSCs), in consultation with the supporting SJA, will ensure the following notification procedures are followed:

(1) The alert/notification must completely and accurately specify what data was compromised and the steps those potentially affected should take to protect themselves against criminal activity.

(2) When the identities of potentially affected personnel are known, **only** those individuals will be alerted to the incident.

(3) When the identity of persons is unknown, **all** whose information may have been compromised will be notified.

(4) The alert will be provided to each person whose information was or might have been compromised by first class mail and also be disseminated through AKO and other means of communication available to the command. Very large scale breach alerts will be passed to the command public affairs officer for dissemination to the media.

(5) That the affected organization will solicit positive confirmation from affected individuals that they have been notified and their replies are kept on file. Provide a toll free telephone number/website to receive feedback from affected personnel.

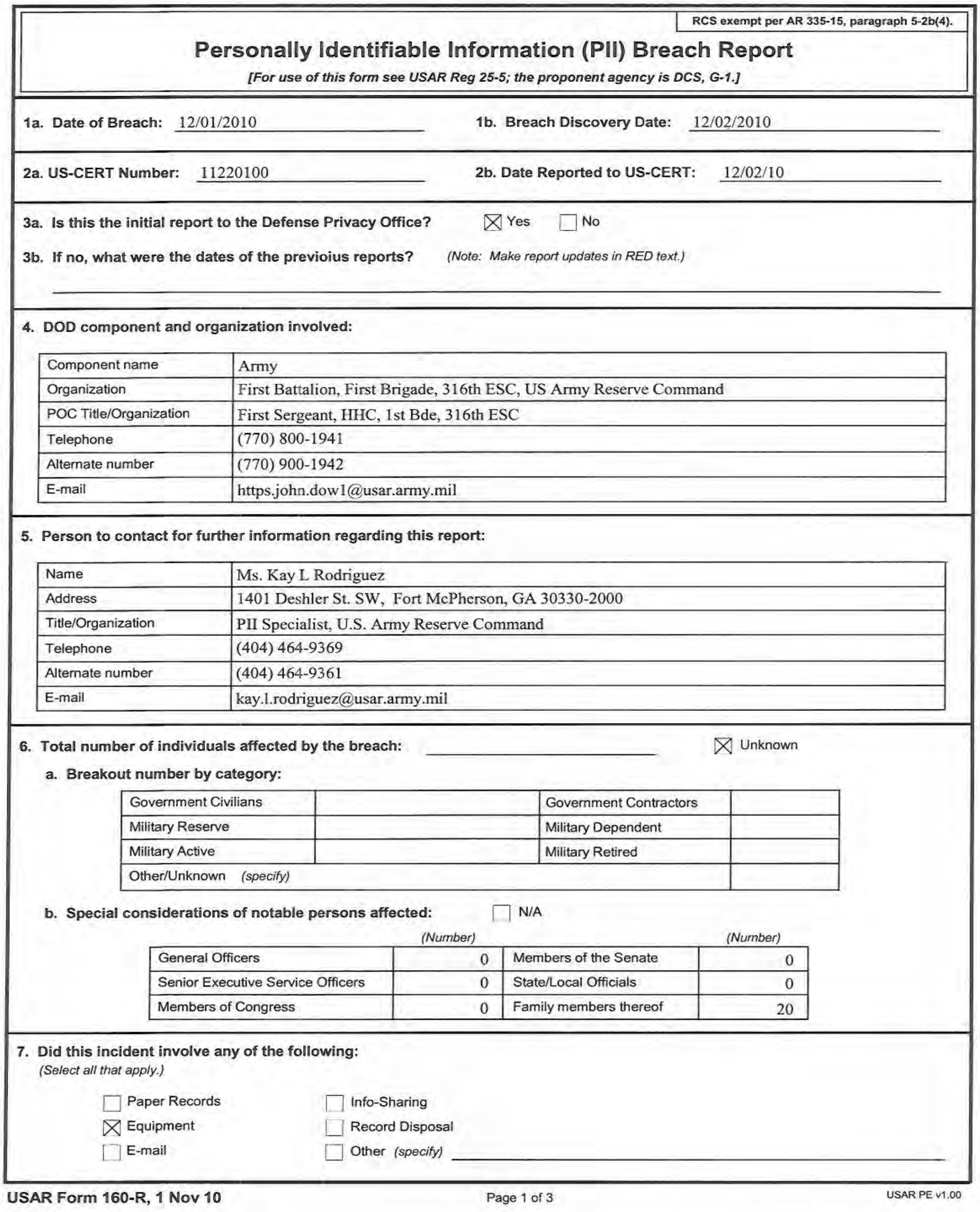
(6) A report will be provided, via the AROC, to the USARC, ATTN: Chief of Staff, indicating the names of individuals notified.

(7) The alert will describe the circumstances surrounding the breach; state what elements of data were lost, such as social security numbers, home addresses, home phone numbers, pay grades, medical conditions, names and ages of family members, etc., explain what is being done to investigate the incident, mitigate losses, and protection against any further breaches; provide a contact for responding to individual inquiries; and provide the Federal Trade Commission website at http://www.ftc.gov/bcp/edu/microsites/idtheft, for assisting the individuals affected (see section for military).

(8) Alerts at company and lower levels should be prepared by the company commander with copies furnished through the chain of command to the USARC, ATTN: ARRC-PRA-R (Privacy Specialist). The specialist will include breach incidents in a quarterly report to HQDA pursuant to Public Law 110-53, *Implementing Recommendation of the 9/11 Commission Act of 2007*. The MSCs' SJA and the USARC Privacy Specialist can always be called upon for assistance.

(9) Alerts at echelons higher than company will be coordinated with their higher commander, the privacy specialist and SJA at higher echelons of commands, with a copy furnished to HQ, USARC G-1, RMPB, Privacy Specialist, for inclusion in the quarterly report to HQDA.

(10) Alerts for incidents that involve the entire force will be released by HQ USARC as part of an overall response action plan delineated under separate cover.



RCS exempt per AR 335-15, paragraph 5-2b(4).

Personally Identifiable Information (PII) Breach Report

[For use of this form see USAR Reg 25-5; the proponent agency is DCS, G-1.]

1a. Date of Breach: 12/01/2010 **1b. Breach Discovery Date:** 12/02/2010

2a. US-CERT Number: 11220100 **2b. Date Reported to US-CERT:** 12/02/10

3a. Is this the initial report to the Defense Privacy Office? ☒ Yes ☐ No

3b. If no, what were the dates of the previoius reports? *(Note: Make report updates in RED text.)*

4. DOD component and organization involved:

Component name	Army
Organization	First Battalion, First Brigade, 316th ESC, US Army Reserve Command
POC Title/Organization	First Sergeant, HHC, 1st Bde, 316th ESC
Telephone	(770) 800-1941
Alternate number	(770) 900-1942
E-mail	https.john.dow1@usar.army.mil

5. Person to contact for further information regarding this report:

Name	Ms. Kay L Rodriguez
Address	1401 Deshler St. SW, Fort McPherson, GA 30330-2000
Title/Organization	PII Specialist, U.S. Army Reserve Command
Telephone	(404) 464-9369
Alternate number	(404) 464-9361
E-mail	kay.l.rodriguez@usar.army.mil

6. Total number of individuals affected by the breach: ☒ Unknown

a. Breakout number by category:

Government Civilians		Government Contractors	
Military Reserve		Military Dependent	
Military Active		Military Retired	
Other/Unknown *(specify)*			

b. Special considerations of notable persons affected: ☐ N/A

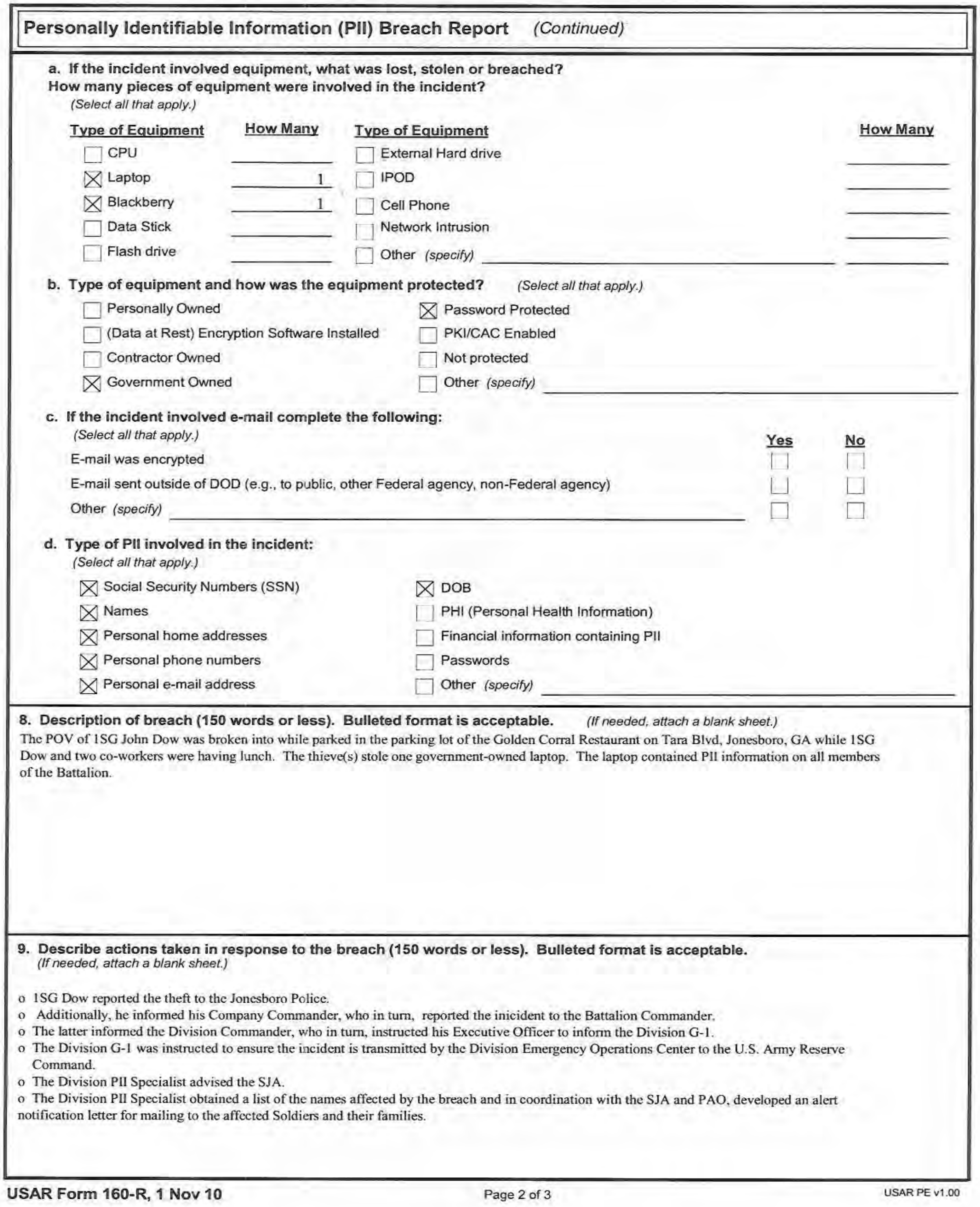
	(Number)		*(Number)*
General Officers	0	Members of the Senate	0
Senior Executive Service Officers	0	State/Local Officials	0
Members of Congress	0	Family members thereof	20

7. Did this incident involve any of the following:
(Select all that apply.)

☐ Paper Records ☐ Info-Sharing
☒ Equipment ☐ Record Disposal
☐ E-mail ☐ Other *(specify)*

USAR Form 160-R, 1 Nov 10 Page 1 of 3 USAR PE v1.00

Figure B-1. Sample USAR Form 160-R, Personally Identifiable Information (PII) Breach Report



Personally Identifiable Information (PII) Breach Report *(Continued)*

a. If the incident involved equipment, what was lost, stolen or breached? How many pieces of equipment were involved in the incident?
(Select all that apply.)

Type of Equipment	How Many	Type of Equipment	How Many
□ CPU		□ External Hard drive	
☒ Laptop	1	□ IPOD	
☒ Blackberry	1	□ Cell Phone	
□ Data Stick		□ Network Intrusion	
□ Flash drive		□ Other *(specify)*	

b. Type of equipment and how was the equipment protected? *(Select all that apply.)*

□ Personally Owned	☒ Password Protected
□ (Data at Rest) Encryption Software Installed	□ PKI/CAC Enabled
□ Contractor Owned	□ Not protected
☒ Government Owned	□ Other *(specify)*

c. If the incident involved e-mail complete the following:
(Select all that apply.)

	Yes	No
E-mail was encrypted	□	□
E-mail sent outside of DOD (e.g., to public, other Federal agency, non-Federal agency)	□	□
Other *(specify)*	□	□

d. Type of PII involved in the incident:
(Select all that apply.)

☒ Social Security Numbers (SSN)	☒ DOB
☒ Names	□ PHI (Personal Health Information)
☒ Personal home addresses	□ Financial information containing PII
☒ Personal phone numbers	□ Passwords
☒ Personal e-mail address	□ Other *(specify)*

8. Description of breach (150 words or less). Bulleted format is acceptable. *(If needed, attach a blank sheet.)*

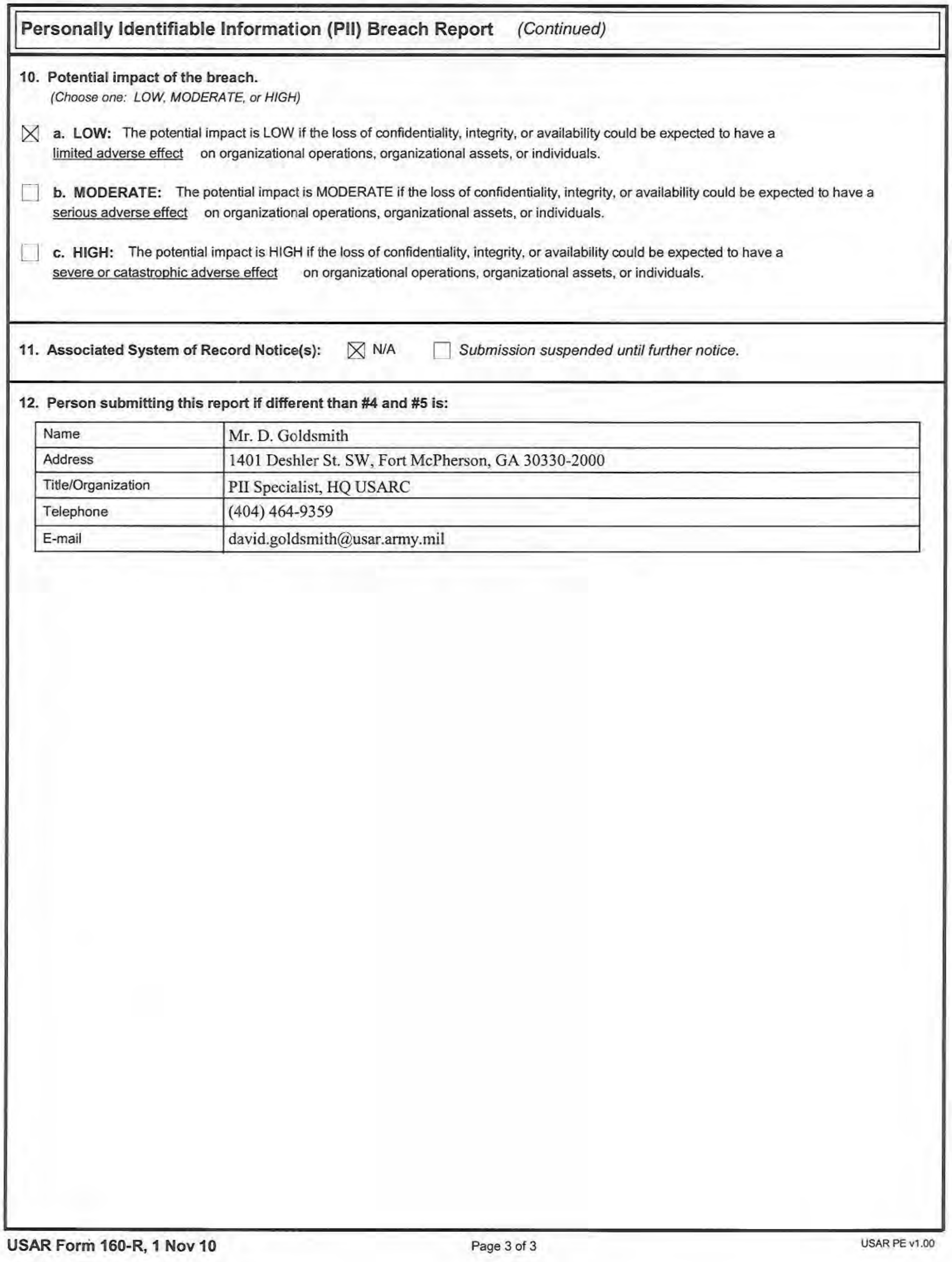
The POV of 1SG John Dow was broken into while parked in the parking lot of the Golden Corral Restaurant on Tara Blvd, Jonesboro, GA while 1SG Dow and two co-workers were having lunch. The thieve(s) stole one government-owned laptop. The laptop contained PII information on all members of the Battalion.

9. Describe actions taken in response to the breach (150 words or less). Bulleted format is acceptable.
(If needed, attach a blank sheet.)

o 1SG Dow reported the theft to the Jonesboro Police.
o Additionally, he informed his Company Commander, who in turn, reported the inicident to the Battalion Commander.
o The latter informed the Division Commander, who in turn, instructed his Executive Officer to inform the Division G-1.
o The Division G-1 was instructed to ensure the incident is transmitted by the Division Emergency Operations Center to the U.S. Army Reserve Command.
o The Division PII Specialist advised the SJA.
o The Division PII Specialist obtained a list of the names affected by the breach and in coordination with the SJA and PAO, developed an alert notification letter for mailing to the affected Soldiers and their families.

USAR Form 160-R, 1 Nov 10 Page 2 of 3 USAR PE v1.00

Figure B-1 Continued. Sample USAR Form 160-R, Personally Identifiable Information (PII) Breach Report



Personally Identifiable Information (PII) Breach Report *(Continued)*

10. Potential impact of the breach.
(Choose one: LOW, MODERATE, or HIGH)

☒ **a. LOW:** The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

□ **b. MODERATE:** The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

□ **c. HIGH:** The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11. Associated System of Record Notice(s): ☒ N/A □ *Submission suspended until further notice.*

12. Person submitting this report if different than #4 and #5 is:

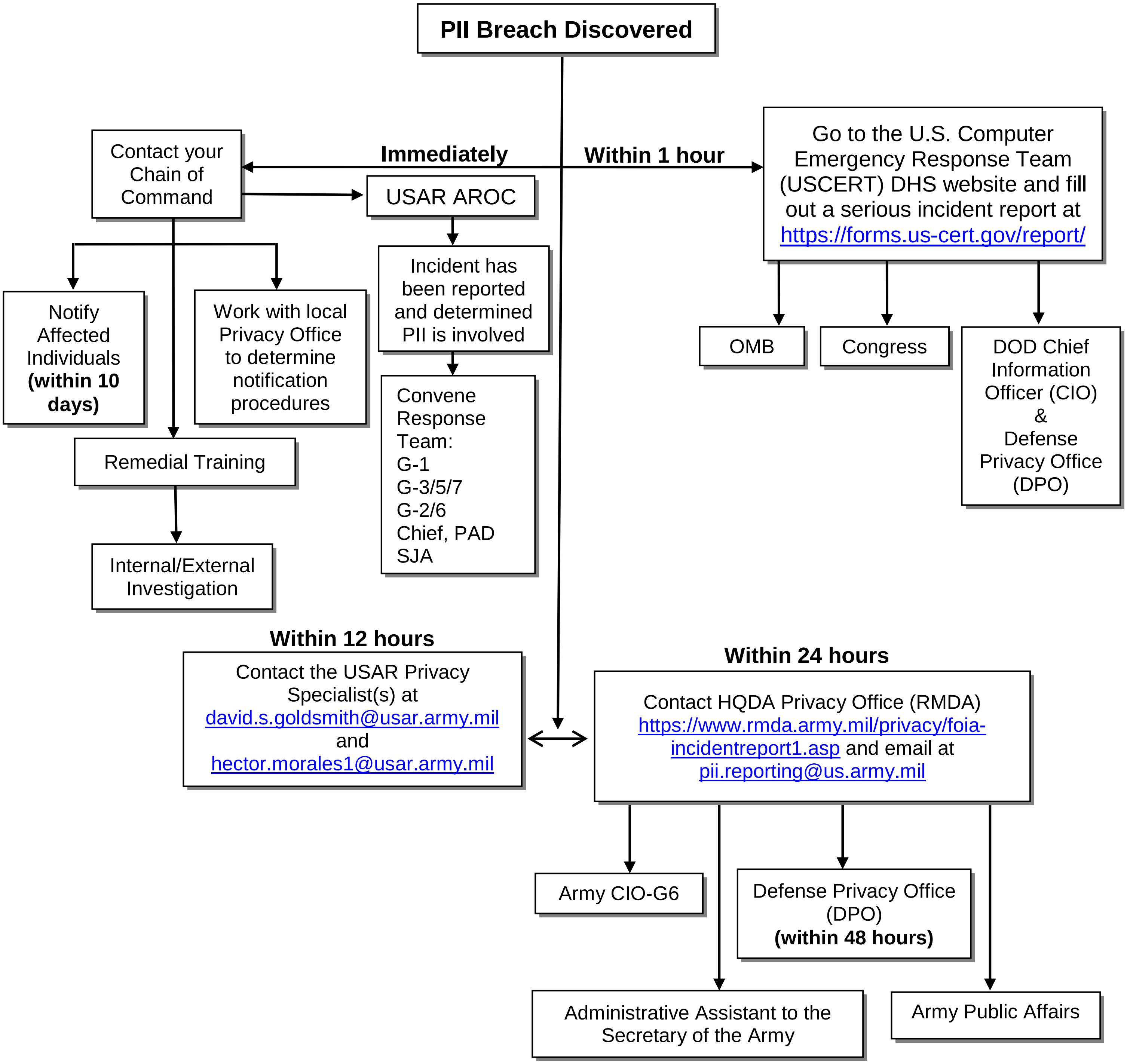
Name	Mr. D. Goldsmith
Address	1401 Deshler St. SW, Fort McPherson, GA 30330-2000
Title/Organization	PII Specialist, HQ USARC
Telephone	(404) 464-9359
E-mail	david.goldsmith@usar.army.mil

USAR Form 160-R, 1 Nov 10 Page 3 of 3 USAR PE v1.00

Figure B-1 Continued. Sample USAR Form 160-R, Personally Identifiable Information (PII) Breach Report

Appendix C
PII Breach Flow Chart

A breach occurs when an actual or possible loss of control, unauthorized disclosure, or access, occurs regardless of whether data was exposed internally or externally.



PII Breach Discovered

Immediately

Contact your Chain of Command

USAR AROC

Incident has been reported and determined PII is involved

Convene Response Team:
G-1
G-3/5/7
G-2/6
Chief, PAD
SJA

Notify Affected Individuals **(within 10 days)**

Work with local Privacy Office to determine notification procedures

Remedial Training

Internal/External Investigation

Within 1 hour

Go to the U.S. Computer Emergency Response Team (USCERT) DHS website and fill out a serious incident report at https://forms.us-cert.gov/report/

OMB

Congress

DOD Chief Information Officer (CIO) & Defense Privacy Office (DPO)

Within 12 hours

Contact the USAR Privacy Specialist(s) at david.s.goldsmith@usar.army.mil and hector.morales1@usar.army.mil

Within 24 hours

Contact HQDA Privacy Office (RMDA) https://www.rmda.army.mil/privacy/foia-incidentreport1.asp and email at pii.reporting@us.army.mil

Army CIO-G6

Defense Privacy Office (DPO) **(within 48 hours)**

Administrative Assistant to the Secretary of the Army

Army Public Affairs

Glossary

Section I
Abbreviations

AKO
Army knowledge Online

AROC
Army Reserve Operations Center

CD/DVD
compact disk/digital video disk

CIO
Chief Information Officer

CPU
computer processing unit

DA
Department of the Army

DOB
date of birth

DOD
Department of Defense

DPO
Defense Privacy Office

Email
Electronic Mail

FOUO
For Official Use Only

MSC
Major Subordinate Command

OCAR
Office of the Chief Army Reserve

OMB
Office of Management and Budget

PHI
personal health information

PII
Personally Identifiable Information

SJA
Staff Judge Advocate

SSN
Social Security Number

USAR
United States Army Reserve

USARC
United States Army Reserve Command

USCERT
United States Army Computer Emergency Response Team

Section II
Term(s)

PII refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.