



DEFENSE CONTRACT AUDIT AGENCY
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

DL

September 27, 2017

DCAA INSTRUCTION
NO. 5410.10

DCAA PRIVACY PROGRAM

Reference: See [Enclosure 1](#)

1. PURPOSE.

a. This instruction provides policies and procedures for the Defense Contract Audit Agency's (DCAA) implementation of 552a of Title 5, United States Code (U.S.C.) (also known and referred to in this directive as "The Privacy Act" (Reference (a)) and Office of Management and Budget (OMB) Circular No. A-130 (Reference (c)) and is intended to promote uniformity within the Agency. It includes procedures for reporting an unauthorized disclosure of personally identifiable information (PII) pursuant to OMB Memorandum M-07-16.

b. This instruction supersedes DCAAI 5010.10, DCAA Privacy Program, dated February 15, 2011.

2. APPLICABILITY. This instruction shall be applicable to all DCAA organizational elements and any DCAA contractor and any employee of such a DCAA contractor when the contractor operates or maintains by contract a DCAA system of records to accomplish an agency function.

3. POLICY. It is DCAA policy that:

a. All personnel will comply with the DCAA Privacy Program and the Privacy Act of 1974.

b. DCAA employees and DCAA contractor employees shall safeguard personal information contained in any information system covered by a system of records notice (SORN) maintained by DCAA organizational elements or contractors and to make that information available to the individual to whom it pertains to the maximum extent practicable.

c. DCAA employees and contractors shall report all incidents of actual or suspected PII compromise (intentional, negligent, internal, external, electronic, or paper), to the DCAA Office of Information Technology (OIT). OIT shall report the incident to the United States Computer Emergency Readiness Team (US-CERT), within the Department of Homeland Security; and to the Defense Privacy and Civil Liberties Division.

d. Pursuant to The Privacy Act, no record will be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution of the United States (referred to in this directive as “the First Amendment,”) except:

- (1) When specifically authorized by statute.
- (2) When expressly authorized by the individual that the record is about.
- (3) When the record is pertinent to and within the scope of an authorized law enforcement activity, including an authorized intelligence or administrative investigation.

e. In DoD 5400.11 (Reference b), DoD has established rules of conduct for DoD personnel and DoD contractors involved in the design, development, operation, or maintenance of any information systems covered by a SORN. DCAA will train all personnel and contractors with respect to such rules, and all DCAA employees and contractors will conduct themselves consistent with the established rules of conduct for safeguarding privacy data.

f. Disclosure of records pertaining to an individual from an information system covered by a SORN is prohibited except with his or her consent or as otherwise authorized by References (b) and (d). When such disclosures occur, the individual may, to the extent authorized by References (b) and (d), obtain a description of such disclosures from the Component system owner.

g. PII collected, used, maintained, or disseminated will be:

(1) Relevant and necessary to accomplish a lawful DCAA purpose required by statute or Executive order.

(2) Collected to the greatest extent practicable directly from the individual. He or she will be informed as to why the information is being collected, the authority for collection, how it will be used, whether disclosure is mandatory or voluntary, and the consequences of not providing that information.

(3) Relevant, timely, complete, and accurate for its intended use.

(4) Protected using appropriate administrative, technical, and physical safeguards to ensure that the PII is safeguarded from compromise or misuse.

h. Individuals are permitted, to the extent authorized by References (b) and (d), to:

(1) Upon request, gain access to records or to any information pertaining to the individual, which is contained in a system of records.

(2) Obtain a copy of such records, in whole or in part.

(3) Correct or amend such records once it has been determined that the records are not accurate, relevant, timely, or complete.

(4) Appeal a denial for a request to access or a request to amend a record.

i. DCAA personnel involved in the design, development, operation, or maintenance of any system of records shall adhere to the requirements of this instruction, DCAAR 8500.1, and The Privacy Act: An Employee Guide to Privacy. System of records notices (SORNs) and notices of proposed or final rulemaking are published in the Federal Register (FR), and reports are submitted to Congress and OMB, in accordance with References (b) through (d). Information about an individual maintained in a new system of records will not be collected until the required SORN publication and review requirements are satisfied.

j. Individuals shall be advised of their right to appeal any denial of access or amending of any record pertaining to them, and their right to file a statement of disagreement if amendment of a record is denied.

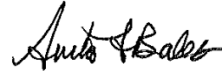
4. RESPONSIBILITIES. See [Enclosure 2](#).

5. INFORMATION COLLECTION REQUIREMENTS.

a. Reporting requirements are prescribed and detailed in DoD 5400.11-R.

6. RELEASABILITY. UNLIMITED. This Issuance is approved for public release and is available on the Intranet website.

7. EFFECTIVE DATE. This instruction is effective immediately.



Anita F. Bales
Director

Enclosures

1. References
2. Responsibilities
3. Procedures
4. Privacy Act Violations
5. Reporting Flowchart for Actual or Suspected PII Compromise
6. Breach of Personally Identifiable Information (PII) Report
7. Risk Assessment Guide

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES	6
ENCLOSURE 2: RESPONSIBILITIES	7
DIRECTOR, DCAA	7
GENERAL COUNSEL, DCAA	7
THE DCAA PRIVACY OFFICER	7
REGIONAL DIRECTORS, CORPORATE AUDIT DIRECTORS, AND HEADQUARTERS ASSISTANT DIRECTORS	9
THE CHIEF INFORMATION OFFICER (CIO)	9
ORGANIZATIONAL PRIVACY POINTS OF CONTACT	10
MANAGERS, FIELD AUDIT OFFICES	10
DCAA EMPLOYEES	10
ENCLOSURE 3: PROCEDURES	12
ENCLOSURE 4: PRIVACY ACT VIOLATIONS	14
ENCLOSURE 5: REPORTING FLOWCHART FOR ACTUAL OR SUSPECTED PII COMPROMISE	15
ENCLOSURE 6: BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT	16
ENCLOSURE 7: RISK ASSESSMENT GUIDE	19
GLOSSARY	23
DEFINITIONS	23
TABLE	
RISK ASSESSMENT GUIDE	19
FIGURES	
1. REPORTING FLOWCHART FOR ACTUAL OR SUSPECTED PII COMPROMISE	15
2. DD FORM 2959	16

ENCLOSURE 1

REFERENCES

- (a) Title 5, United States Code, Section 552a.
- (b) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
- (c) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1996
- (d) DoD 5400.11-R, DoD Privacy Program, May 14, 2007.
- (e) DCAAI 5410.8, DCAA Freedom of Information Act Program, September 27, 2016.
- (f) Office of Management & Budget (OMB) Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.
- (g) DCAAI 8500.1, Information Assurance (IA) Program, September 24, 2009.
- (h) DoDI 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, July 14, 2015.
- (i) The Privacy Act: An Employee Guide to Privacy, March 1, 2016.
- (j) Office of Management & Budget (OMB) Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.
- (k) DCAAM 8500.3, DCAA Computer Incident Response Plan, April 1, 2013

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DCAA

- a. Establishes and supports an effective DoD Privacy Program.
- b. Establishes appropriate administrative, physical, and technical safeguards and procedures prescribed in the DoD Privacy Program guidance.

2. GENERAL COUNSEL, DCAA

- a. Serves as the Component Senior Official for Privacy (CSOP) to support the Senior Agency Official for Privacy (SAOP) for DoD.
- b. Establishes, issues, and updates policies for the DCAA Privacy Program; monitors compliance with this instruction; and provides policy guidance for the DCAA Privacy Program.
- c. Oversees and provides strategic direction for the DCAA Privacy Program.
- d. Provides advice and assistance on all legal matters related to the administration of the DoD Privacy Program.
- e. Serves as the sole appellate authority for appeals to decisions of initial denial authorities.
- f. Designates an Agency Privacy Officer, as a single point of contact, to coordinate on matters concerning Privacy Act policy.
- g. Consults with DoD General Counsel on final denials that are inconsistent with decisions of other DoD components, involve issues not previously encountered, or raise new or significant legal issues of potential significance to other Government agencies.
- h. Coordinates Privacy Act litigation with the Department of Justice.
- i. Ensures that the Director, DCAA and Deputy Director, DCAA are fully apprised of all significant developments with the DCAA Privacy Program.

3. The DCAA PRIVACY OFFICER, under the direction of the General Counsel, shall:

- a. Manage the DCAA Privacy Program in accordance with this instruction and applicable DCAA policies as well as DoD and Federal regulations.

- b. Provide guidelines for managing, administering, and implementing the DCAA Privacy Program.
- c. Implement and administer the DCAA Privacy Program.
- d. Make the initial determination to deny an individual's written Privacy Act request for access to or amendment of documents filed in any Agency system of records.
- e. Ensure that the collection, maintenance, use, or dissemination of records containing PII is in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.
- f. Review and coordinate proposed PIAs to confirm that privacy implications have been identified and evaluated to ensure the proper balance is struck between an individual's privacy and the Agency's information requirements .
- g. Prepare promptly any required new, amended, or altered SORNs for records subject to the Privacy Act and submit them to the Defense Privacy and Civil Liberties Division for subsequent publication in the Federal Register.
- h. Provide advice and assistance to the Assistant Directors, Regional Directors, Corporate Audit Directorates, the Chief Information Officer, and the regional privacy points of contact, as required, in the discharge of their responsibilities.
- i. Prepare and submit all reporting elements as required by DoD 5400.11-R, DoD Privacy Program .
- j. Arrange required training on the DCAA Privacy Program for Agency personnel.
- k. Report all incidents of compromised PII to the Defense Privacy and Civil Liberties Division within 48 hours.
- l. Assess the likely risk and level of harm to the individuals whose personal information was compromised to determine whether notification should be given and the nature of the notification to the affected individuals. Notification should be made on a case by case basis in accordance with procedures. A determination to notify affected individuals shall be made as soon as possible, but not later than 10 work days after the loss, theft, or compromise is discovered and the identities of the affected individuals ascertained. When notification is not made within the 10 work day period, DCAA shall inform the Deputy Secretary of Defense why notice was not provided within the 10 work day period.

4. REGIONAL DIRECTORS, CORPORATE AUDIT DIRECTORS, and HEADQUARTERS ASSISTANT DIRECTORS, are responsible for:

- a. Providing overall management of the Privacy Program within their respective organization and designating a privacy point of contact within their organization.
- b. Reviewing all instructions or other policy and guidance issuances for which they are the proponent to ensure consistency with the provisions of the DCAA Privacy Program specified in this instruction.
- c. Forwarding to the DCAA privacy officer any Privacy Act requests received so that the request may be administratively controlled and processed.
- d. For incidents of actual or suspected PII compromise, assisting in investigating, taking corrective actions, and providing updates to Operations and the DCAA privacy officer in accordance with reporting procedures

5. The CHIEF INFORMATION OFFICER (CIO) is responsible for:

- a. Completing actions in accordance with DoD Privacy Impact Assessment Guidance, ensuring that personal information in electronic form is only acquired and maintained when necessary, and that the supporting information technology (IT) that is being developed and used protects and preserves the privacy of individuals.
- b. Providing for the planning, coordination, integration, and oversight of all DCAA information assurance (IA) activities.
- c. Serving as the Agency's Privacy Impact Assessment (PIA) review official.
- d. Ensuring that new or modified IT systems that collect, maintain, or disseminate information in identifiable form and/or new electronic collections of information in identifiable form, for 10 or more persons (excluding DoD personnel), have a PIA performed by the office responsible for the IT system. (Refer to Reference H for the DoD PIA format.)
- e. Ensuring PIAs are completed before developing, procuring, or modifying the IT system; and acquiring appropriate coordination with the office submitting the request, the IA official, and the DCAA Records Manager.
- f. Forwarding all PIAs for IT systems and projects to OMB.
- g. Posting approved PIAs or summary PIAs on the Agency's public web site.
- h. Reporting any potential or actual PII compromise to US-CERT WITHIN ONE HOUR of Agency knowledge of the incident, and notifying the DCAA Privacy Officer.

6. Organizational PRIVACY POINTS OF CONTACT shall:

- a. Assist in the implementation and administration of the DCAA Privacy Program throughout their respective organization.
- b. Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information is done in accordance with this instruction and in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.
- c. Upon receipt of an Incident Report related to actual or suspected PII compromise, complete and submit a Breach of Personally Identifiable Information (PII) Report (refer to [Enclosure 6](#)) to the DCAA Privacy Officer in accordance with reporting procedures; and continue to update the DCAA Privacy Officer until the investigation is closed and a final report is issued.

7. MANAGERS, FIELD AUDIT OFFICES, shall:

- a. Ensure that their staff follows the provisions of this instruction in processing requests for records and in reporting incidents of actual or suspected PII compromise.
- b. Forward to the DCAA Privacy Officer any Privacy Act requests received so that the request may be administratively controlled and processed.
- c. Provide recommendations to the DCAA privacy officer regarding the releasability of DCAA records to individuals, along with the responsive documents.

8. DCAA employees shall:

- a. Not disclose any personal information contained in any system of records, except as authorized by this instruction.
- b. Not maintain any official records that are retrieved by name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual without identifying the statute or Executive Order authorizing the collection of such information and ensuring that a notice for the system of records has been published in the Federal Register.
- c. Report any disclosures of personal information from a system of records.
- d. Report the use of any system of records not authorized by this instruction to the appropriate Privacy Act officials for action.

e. Immediately report any incident of actual or suspected PII compromise in accordance with reporting procedures described herein.

ENCLOSURE 3PROCEDURES

a. Procedures for processing material in accordance with the Privacy Act of 1974 are outlined in reference b .

b. DCAA is required to report, WITHIN ONE HOUR OF AGENCY KNOWLEDGE OF, all incidents (intentional, negligent, internal, and external) of actual or suspected, electronic or paper, PII compromise to the United States Computer Emergency Readiness Team (US-CERT), within the Department of Homeland Security; and to the Defense Privacy and Civil Liberties Division within 48 hours, as follows:

(1) Employees and contractor personnel must IMMEDIATELY report any incident of actual or suspected PII compromise, electronic or paper, to their supervisor, or higher level if supervisor is unavailable.

(2) The supervisor and or employee must immediately contact OIT at (703) 767-2238. If calling after hours, leave a detailed message. If unsure whether PII has been compromised, report the incident. Be aware that contractor proprietary data may contain PII.

(3) OIT must report any potential or actual compromise to US-CERT and also notify the DCAA privacy officer.

(4) WITHIN 24 HOURS, the employee or supervisor must submit an Incident Report (Appendix A, DCAAM 8500.3) to OIT (refer to DCAAM 8500.3, DCAA Computer Incident Response Plan) and their cognizant Privacy Officer or the DCAA Privacy Officer.

(5) The cognizant privacy point of contact must IMMEDIATELY submit a Breach of Personally Identifiable Information (PII) Report (refer to [Enclosure 6](#)), with as much information as is known, to the DCAA Privacy Officer, who reports the incident to the Defense Privacy and Civil Liberties Division WITHIN 48 HOURS. If there is a continuing investigation, the cognizant privacy point of contact reports additional information as it becomes known.

c. A decision must be made regarding whether or not to notify individuals whose personal information is compromised, as follows:

(1) The DCAA Privacy Officer must assess the likely risk and level of harm to the individuals affected by the breach to determine whether notification should be given and the nature of the notification to the affected individuals. Notification is not always necessary or desired; appropriate notification should be made on a case by case basis considering the five factors listed in [Enclosure 7](#), Risk Assessment Guide. The Risk Assessment Guide must be used to make determinations of risk of harm associated with a breach (loss, theft, or compromise) of PII. The notification will be sent out by the cognizant Region or CAD from which the breach originated.

(2) A determination to notify affected individuals must be made as soon as possible, but not later than 10 work days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained. When notification is not made within the 10 work day period, DCAA must inform the Deputy Secretary of Defense why notice was not provided within the 10 work day period.

(3) The notification must be made in writing (memorandum or e-mail), using the most effective means for the situation, and be concise, conspicuous, and written in plain language. The notice must include the following elements:

(a) A brief description of what happened, including the date(s) of the breach and of its discovery.

(b) To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, social security number, date of birth, home address, account number, disability code, etc.).

(c) A statement whether the information was encrypted or protected by other means if it is determined that such information would be beneficial and would not compromise the security of the system.

(d) What steps individuals should take to protect themselves from potential harm, if any.

(e) What DCAA is doing to investigate the breach, to mitigate losses, and to protect against further breaches.

(f) Who affected individuals should contact at DCAA for more information, including a phone number, e-mail address, and postal address.

ENCLOSURE 4

PRIVACY ACT VIOLATIONS

Penalties can be assessed against individuals or agencies for Privacy Act violations (reference a).

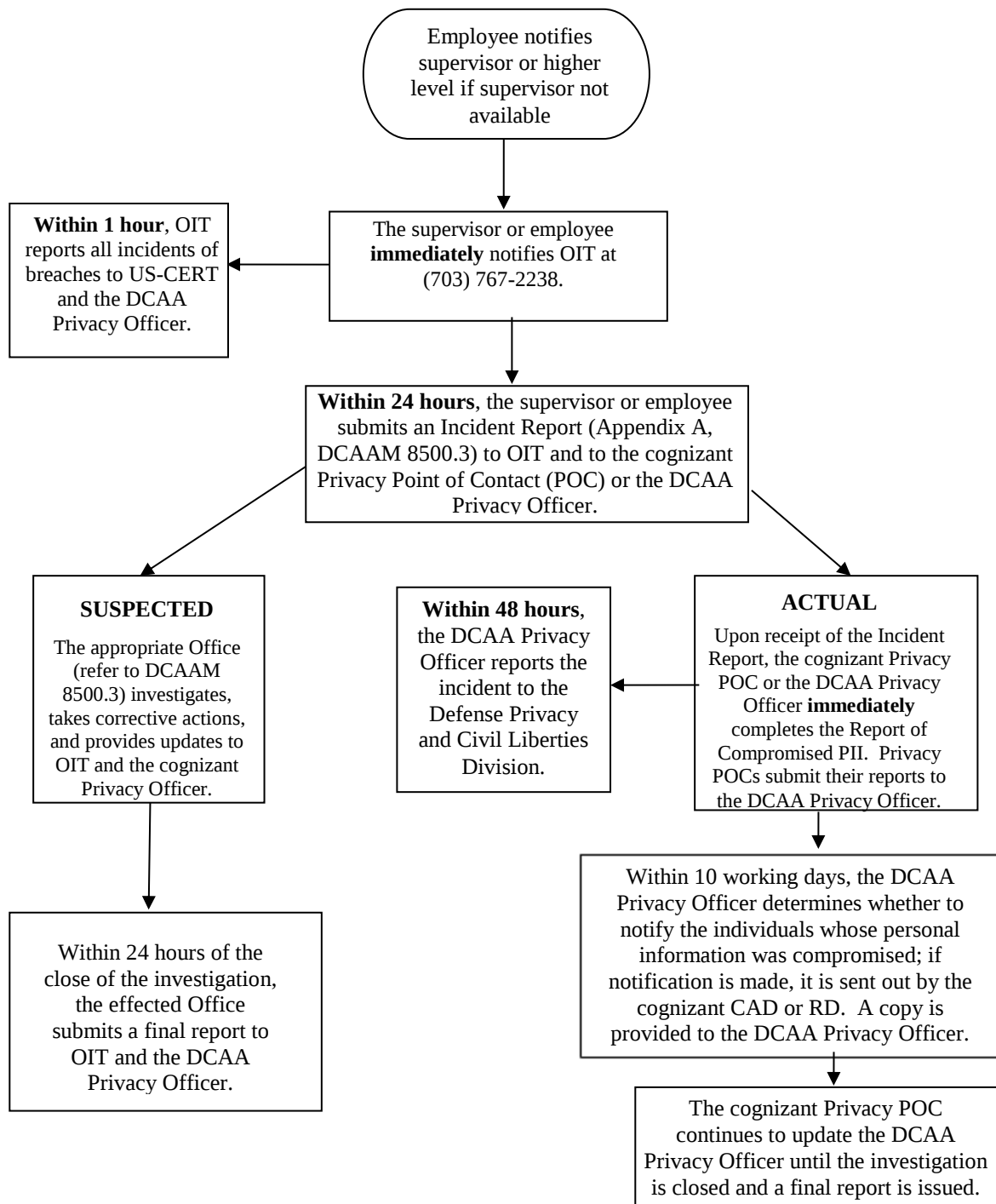
a. Violations can result in a misdemeanor criminal charge and fine of up to \$5,000 for any employee who knowingly and willfully discloses personal information to a person not authorized access; knowingly and willfully requests or obtains personal information under false pretenses; or maintains an unauthorized System of Records (i.e., collects and maintains personal information on individuals that is not covered by an existing System of Records).

b. The Privacy Act also imposes civil penalties on agencies that unlawfully refuse to amend a record; unlawfully refuse to grant access to records; fail to maintain accurate, relevant, timely, and complete data; or fail to comply with any Privacy Act provision or agency rule that results in an adverse effect. Penalties include payment of actual damages and reasonable attorney fees.

ENCLOSURE 5

REPORTING FLOWCHART FOR ACTUAL OR SUSPECTED PII COMPROMISE

Figure 1. REPORTING FLOWCHART FOR ACTUAL OR SUSPECTED PII COMPROMISE



ENCLOSURE 6BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORTFigure 2. DD FORM 2959.

BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT			
INITIAL REPORT		UPDATED REPORT	
Date: (MM/DD/YYYY)		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, FEB 2013

Adobe Designer 9.0

Figure 2. DD FORM 2259, Continued

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 (2) If Yes, notification date (MM/DD/YYYY) (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		(1) If Yes, were they notified within 10 working days? ☐ Yes ☐ No (3) If Yes, number of individuals notified: (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? ☐ (c) Other (Specify): ☐ Yes ☐ No	
5. SELECT ALL THE FOLLOWING THAT APPLY TO THIS BREACH					
a. PAPER DOCUMENTS/RECORDS (If selected, provide additional detail)			b. EQUIPMENT (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):			☐ (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 ☐ (2) Cell phone ☐ (3) Personal Digital Assistant		☐ (4) MP3 player ☐ (5) Printer/Copier/Fax/Scanner ☐ (6) Desktop computer		☐ (7) Flash drive/USB stick/other removable media ☐ (8) External hard drive ☐ (9) Other (Specify):	
d. EMAIL (If selected, provide additional detail)			e. INFO DISSEMINATION (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			☐ (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), FEB 2013

Figure 2. DD FORM 2259, Continued

INSTRUCTIONS FOR COMPLETING DD FORM 2959, BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT	
Select Initial, Updated, or After Action Report and enter the date.	
1. GENERAL INFORMATION.	
a. Date of Breach. Enter the date the breach occurred. If the specific date cannot be determined, enter an estimated date and provide further explanation in the notes section of the report.	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. Summarize steps taken to mitigate actual or potential harm to the individuals affected and the organization. For example, training, disciplinary action, policy development or modification, information systems modifications. List any findings resulting from the investigation of the breach.
b. Date Breach Discovered. Enter the date the breach was initially discovered by a DoD employee, military member, or DoD contractor.	3.a. NUMBER OF INDIVIDUALS AFFECTED. For each category of individuals listed, enter the number of individuals affected by the breach. Do not include an individual in more than one category.
c. Date reported to US-CERT. Breaches must be reported to US-CERT within 1 hour of discovery. Enter the date reported to US-CERT.	b. Were affected individuals notified? Check box "Yes" or "No". If the individuals affected will not receive a formal notification letter about the breach, select "No" and enter an explanation of why the Component determined notification was not necessary in 3.b.(4). If additional space is needed for this justification, continue text in 6.c., Additional Notes.
d. US-CERT Number. Enter the number assigned by US-CERT when the breach was reported.	(1) If affected individuals were notified, were they notified within 10 working days? Check "Yes" or "No".
e. Component Internal Tracking Number (if applicable). If your component uses an internal tracking number, enter the number assigned.	(2) If the affected individuals will be notified of the breach, provide the date the notification letters will be sent.
f. Breach Involved (click to select). Select from the drop-down list - Email, Info Dissemination, Paper Records, or Equipment.	(3) - (4) If "Yes", list the number of individuals notified. If the number of individuals notified differs from total number of individuals affected, explain why in 3.b.(4).
g. Type of Breach (click to select). Select from the drop-down list - Theft, Loss, or Compromise.	(5) Was credit monitoring offered? Select "Yes" or "No".
h. Cause of Breach (click to select). Select from the drop-down list the predominate cause of the breach - Theft, Failure to Follow Policy, Computer Hacking, Social Engineering, Equipment Malfunction, Failure to Safeguard Government Equipment or Information, Improper Security Settings, or Other.	Note: This is a risk of harm based decision to be made by the DoD Component.
i. - j. Component. Select from the drop-down list. After you select your Component, enter the Office/Name in block 1.j (i.e., if "OSD/JS" is the Component selected, an example of the Office would be "TMA").	(6) If "Yes", enter the number of individuals offered credit monitoring.
k. - s. Point of Contact for Further Information. Enter the requested information for the person to be contacted if DPCLC requires additional details regarding the breach.	4. PERSONALLY IDENTIFIABLE INFORMATION (PII) INVOLVED IN THIS BREACH. Select all that apply. If Financial Information is selected, provide additional details.
2.a. DESCRIPTION OF BREACH (Up to 150 words, bullet format acceptable). Note: Do not include PII or classified information. Summarize the facts or circumstances of the theft, loss or compromise of PII as currently known, including:	5. SELECT ALL THE FOLLOWING THAT APPLY TO THIS BREACH. Check at least one box from the options given. If you need to use the "Other" option, you must specify other equipment involved.
- the description of the parties involved in the breach; - the physical or electronic storage location of the data at risk; - if steps were immediately taken to contain the breach; - whether the breach is an isolated incident or a systemic problem; - who conducted the investigation of the breach; and - any other pertinent information.	a. Paper Documents/Records. If you choose Paper Documents/Records, answer each associated question by selecting from the drop-down options.
	b. - c. Equipment. If you choose Equipment, answer the associated questions by selecting from the drop-down options. Enter a number in the empty field indicating how many pieces of each type of equipment were involved in the breach. If "Other", you will need to specify what type of equipment was involved.
	d. - e. Email and Info Dissemination. If Email or Info Dissemination is selected, choose either "Yes" or "No" for all of the questions.
	6.a. TYPE OF INQUIRY. Select the type of inquiry conducted as a result of the breach. If the inquiry type is "Other", please describe.
	b. Impact Determination. (Component Privacy Official or designee use only.) Select one: What is the overall risk level associated with this breach? Risk is determined by considering the likelihood that the PII can be accessed by an unauthorized person and assessing the impact to the organization and individual if the PII is misused.
	c. Additional Notes. This field can be used to convey additional information.

DD FORM 2959 (INSTRUCTIONS, FEB 2013)

ENCLOSURE 7RISK ASSESSMENT GUIDETable 1. RISK ASSESSMENT GUIDE.

No	Factor	Risk Determination	Comments
		High: Low or Moderate:	High risk requires notification. Low and moderate risk/harm determinations and the decision whether notification is made rests with the AD, CAD, or RD where the breach occurred.
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 may have or those that could readily identify an individual, i.e., public figure.
	b. Name plus 1 or more personal identifiers (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.
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. No Protection	High	

No	Factor	Risk Determination	Comments
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	Evidence shows that PII has been stolen and could possibly be used to commit ID theft.
	c. Compromise		
	(1a) Within DoD Control	Low	No evidence of malicious intent.
	(1b) Within DoD Control	High	Evidence or possibility of malicious intent.
	(2) Beyond DoD Control	High	Possibility that PII could be used with malicious intent or to commit ID theft.

Explanation of the five factors to consider when assessing the likelihood of risk and/or harm:

1. Nature of the Data Elements Breached. 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, theft of a database containing individuals' names in conjunction with social security numbers, and/or dates of birth may pose a high risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context. 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. 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.

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 only determining factor for whether an agency should provide notification.

3. Likelihood the Information is Accessible and Usable. Upon learning of a breach, agencies should assess the likelihood personally identifiable information 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. Depending upon a 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 compromise may be low to non-existent. In this context, proper protection means encryption has been validated by National Institute of Standards & Technology (NIST).

4. Likelihood the Breach May Lead to Harm.

a. Broad Reach of Potential Harm. The Privacy Act requires agencies to protect 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 compromise 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.

b. Likelihood Harm Will Occur. 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. Social security numbers and account information are useful to committing identify theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients at a clinic for treatment of a contagious disease.

c. In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the Federal Trade Commission may be found at <http://www.identitytheft.gov>.

5. 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 identify theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

GLOSSARY

DEFINITIONS

Compromised Personally Identifiable Information (PII). Compromised PII is the unauthorized disclosure, acquisition, access, or loss of control in situations where unauthorized persons, or authorized persons for an unauthorized purpose, have access or potential access to PII, whether physical or electronic.

Individual. An individual is a citizen of the United States or an alien lawfully admitted for permanent residence.

Personal Identifiable Information (PII). Personal identifiable information is information about an individual that identifies, links, relates, or is unique to or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as PII (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to a specified individual).

Privacy Impact Assessment (PIA). A PIA is an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Record. Any item, collection, or grouping of information about an individual that is maintained by DCAA including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains an individual's name or identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voice print, or photograph.

System of Records Notice (SORN). A group of any records under the control of DCAA from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. These information systems have a system notice published in the Federal Register and are subject to the provisions of this instruction. All other records fall under the provisions of the Freedom of Information Act (FOIA).