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

CM 15 February 2011

DCAA INSTRUCTION
NO. 5410.10

DCAA PRIVACY PROGRAM
(RCS: DD-COMP(A)1379)

References: See Enclosure 1

1. PURPOSE.

a. This instruction provides policies and procedures for the Defense Contract Audit Agency's implementation of the Privacy Act of 1974 and is intended to promote uniformity within the Agency. It includes procedures for reporting an unauthorized disclosure of personally identifying information pursuant to OMB Memorandum M-07-16 (reference h). Refer to Enclosure 4 for the Reporting Flowchart for Actual or Suspected PII Compromise.

b. This instruction supersedes DCAAR 5010.10, DCAA Privacy Program, dated October 24, 2006.

2. APPLICABILITY.

a. This instruction applies to all DCAA organizational elements and takes precedence over all regional regulatory issuances that supplement the DCAA Privacy Program.

b. This instruction shall be made applicable by contract or other legally binding action to contractors whenever a DCAA contract provides for the operation of a system of records or portion of a system of records to accomplish an Agency function.

3. DEFINITIONS.

a. Personal information. Personal 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).

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

c. 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.

d. 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.

e. 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.

f. System of records. 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. Systems of records must 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) (reference c).

4. POLICY. It is DCAA policy that personnel will comply with the DCAA Privacy Program and the Privacy Act of 1974. Strict adherence is necessary to ensure uniformity in the implementation of the DCAA Privacy Program and to create conditions that will foster public trust. It is Agency policy to safeguard personal information contained in any system of records maintained by DCAA organizational elements and to make that information available to the individual to whom it pertains to the maximum extent practicable. DCAA is required to report all incidents of actual or suspected PII compromise (intentional, negligent, internal, external, electronic or paper), to the United States Computer Emergency Readiness Team (US-CERT), within the Department of Homeland Security; and to the Defense Privacy Office. DCAA policy specifically requires that DCAA organizational elements:

a. Collect, maintain, use, and disseminate personal information only when it is relevant and necessary to achieve a purpose required by statute or Executive Order.

b. Collect personal information directly from the individuals to whom it pertains to the greatest extent practical.

c. Inform individuals who are asked to supply personal information for inclusion in any system of records:

(1) The authority for the solicitation.

(2) Whether furnishing the information is mandatory or voluntary.

(3) The intended uses of the information.

(4) The routine disclosures of the information that may be made outside of DoD.

(5) The effect on the individual of not providing all or any part of the requested information.

d. Ensure that records about individuals containing personal information are accurate, relevant, timely, and complete for the purposes for which they are being maintained.

e. Keep no record that describes how individuals exercise their rights guaranteed by the First Amendment to the U.S. Constitution, unless expressly authorized by statute or by the individual to whom the records pertain or is pertinent to and within the scope of an authorized law enforcement activity.

f. Notify individuals whenever records pertaining to them are made available under compulsory legal processes, if such a process is a matter of public record, and to obtain prior written consent to disclosure from the individual, unless the information requested is disclosed to the individual concerned, or is subject to disclosure as a routine use, or may otherwise be disclosed under any exemption established in 5 U.S.C. § 552a(b), or as allowed by other applicable authority.

g. Establish safeguards to ensure the security of personal information and to protect this information from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual.

h. 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 (reference e), and The Privacy Act: An Employee Guide to Privacy (reference g).

i. Assist individuals in determining what records pertaining to them are being collected, maintained, used, or disseminated.

j. Permit individuals access to their personal information maintained in any system of records, and to correct or amend that information, unless an exemption for the system has been properly established.

k. Provide to an individual, upon request, an accounting of all disclosures of the information pertaining to them except when disclosures are made:

(1) To DoD personnel in the course of their official duties.

(2) Under DoD 5400.11-R (reference b).

(3) As stated in the system notice or under DoD Blanket Routine Uses.

(4) To another agency or to an instrumentality of any governmental jurisdiction within or under control of the United States conducting law enforcement activities authorized by law.

l. Advise individuals of their right to appeal any denial of access to or amendment of any record pertaining to them, and their right to file a statement of disagreement if amendment of a record is denied.

m. Ensure the reporting of all incidents (intentional, negligent, internal, and external) of actual or suspected, electronic or paper, PII compromise in accordance with DCAA reporting procedures.

5. RESPONSIBILITIES.

a. Headquarters.

(1) The Assistant Director, Resources has overall responsibility for the DCAA Privacy Program and will serve as the sole appellate authority for appeals to decisions of initial denial authorities.

(2) Under the direction of the Assistant Director, Resources, the Chief, Administrative Management Division shall:

(a) Establish, issue, and update policies for the DCAA Privacy Program; monitor compliance with this instruction; and provide policy guidance for the DCAA Privacy Program.

(b) Resolve conflicts that may arise regarding implementation of DCAA Privacy Program policy.

(c) Designate an Agency privacy adviser, as a single point of contact, to coordinate on matters concerning Privacy Act policy.

(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. This authority cannot be delegated.

(3) The DCAA privacy adviser under the supervision of the Chief, Administrative Management Division 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 at Headquarters.

(d) Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information 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.

(e) 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.

(f) Prepare promptly any required new, amended, or altered system notices for systems of records subject to the Privacy Act and submit them to the Defense Privacy Office for subsequent publication in the Federal Register.

(g) Prepare the annual Privacy Act Report as required by DoD 5400.11-R, DoD Privacy Program.

(h) Conduct training on the DCAA Privacy Program for Agency personnel.

(i) Report all incidents of compromised PII to the Defense Privacy Office within 48 hours.

(4) Heads of Principal Staff Elements are responsible for:

(a) Reviewing all instructions or other policy and guidance issuances for which they are the proponent to ensure consistency with the provisions of this instruction.

(b) Ensuring that the provisions of this instruction are followed in processing requests for records located in systems of records.

(c) Forwarding to the DCAA privacy adviser any Privacy Act requests received directly so that the request may be administratively controlled and processed.

(d) Ensuring the prompt review of all Privacy Act requests and, when required, coordinating those requests with other organizational elements.

(e) Providing recommendations to the DCAA privacy adviser regarding the releasability of DCAA records to individuals, along with the responsive documents.

(f) Providing the appropriate documents, along with a written justification for any denial, in whole or in part, of a request for records to the DCAA privacy adviser (reference b, paragraph C3.2). The portions of the documents to be excised should be bracketed in red pencil, and the specific exemption or exemptions cited that provide the basis for denying the requested records.

(g) For incidents of actual or suspected PII compromise:

1. Investigating, taking corrective actions, and providing updates to Operations and cognizant privacy officer in accordance with reporting procedures; within 24 hours of the close of the investigation, submits a final report to Operations and the cognizant privacy officer.

2. Assessing 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. 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 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.

(5) The Chief Information Officer (CIO) is responsible for:

(a) Completing actions in accordance with DoD Privacy Impact Assessment Guidance (reference f), 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 (reference e).

(c) Serving as the Agency's 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 (reference d). (Refer to Enclosure 3 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 Chief, Administrative Management Division, Headquarters.

(f) Forward all PIAs for IT systems and projects to OMB.

(g) Post 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 adviser.

(6) The General Counsel is responsible for:

(a) Ensuring uniformity is maintained in the legal position, and the interpretation of the Privacy Act (reference a), DoD 5400.11-R (reference b), and this instruction.

(b) Consulting 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.

(c) Providing advice and assistance to the Assistant Director, Resources; regional directors; the Chief Information Officer; and the regional privacy officer, through the DCAA privacy adviser, as required, in the discharge of their responsibilities.

(d) Coordinating Privacy Act litigation with the Department of Justice.

(e) Coordinating on Headquarters denials of initial requests and appeals.

b. Regional Directors are responsible for:

(1) Providing overall management of the Privacy Program within their respective regions; and providing direction to the appropriate regional manager, who is responsible for the management and staff supervision of the program and for designating a regional privacy officer.

(2) As designee of the Director, making 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. This authority cannot be delegated.

(3) For incidents of actual or suspected PII compromise, are responsible for:

(a) Investigating, taking corrective actions, and providing updates to Operations and cognizant privacy officer in accordance with reporting procedures; within 24 hours of the close of the investigation, submits a final report to Operations and the cognizant privacy officer.

(b) Assessing 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. 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 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 privacy officers shall:

(a) Implement and administer the DCAA Privacy Program throughout the region.

(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) Prepare input for the annual Privacy Act Report when requested by the DCAA privacy adviser.

(d) Conduct training on the DCAA Privacy Program for regional and FAO personnel.

(e) Provide recommendations to the regional director through the appropriate regional manager regarding the releasability of DCAA records to individuals.

(f) Upon receipt of an Incident Report (reference i) related to actual or suspected PII compromise, complete and submit a Report of Potentially Compromised PII (refer to Enclosure 5) to the DCAA privacy advisor in accordance with reporting procedures; and continue to update the DCAA privacy advisor until the investigation is closed and a final report is issued.

(5) Managers, Field Audit Offices (FAOs), shall:

(a) Ensure that their staff follow the provisions of this instruction in processing requests for records and in reporting incidents of actual or suspected PII compromise.

(b) Forward to the regional privacy officer any Privacy Act requests received so that the request may be administratively controlled and processed.

(c) Ensure the prompt review of all Privacy Act requests and, when required, coordinate those requests with other organizational elements.

(d) Provide recommendations to the regional privacy officer regarding the releasability of DCAA records to individuals, along with the responsive documents.

(e) Provide the appropriate documents, along with a written justification for any denial, in whole or in part, of a request for records to the regional privacy officer (reference b, paragraph C3.2). The portions of the documents to be excised should be bracketed in red pencil, and the specific exemption or exemptions cited that provide the basis for denying the requested records.

c. DCAA employees shall:

(1) Not disclose any personal information contained in any system of records, except as authorized by this instruction.

(2) 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.

(3) Report any disclosures of personal information from a system of records.

(4) Report the use of any system of records not authorized by this instruction to the appropriate Privacy Act officials for action.

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

6. PROCEDURES.

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 Office within 48 hours, as follows:

(1) Employees and contractor personnel must IMMEDIATLEY 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 Operations 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) Operations must report any potential or actual compromise to US-CERT and also notify the DCAA privacy advisor.

(4) WITHIN 24 HOURS, the employee or supervisor must submit an Incident Report (Appendix A, DCAAP 8500.3) to Operations (refer to DCAAP 8500.3, DCAA Computer Incident Response Plan) and their cognizant privacy officer.

(5) The cognizant privacy officer must IMMEDIATELY submit a Report of Potentially Compromised PII (refer to Enclosure 5), with as much information as is known, to the DCAA privacy advisor, who reports the incident to the Defense Privacy Office WITHIN 48 HOURS. If there is a continuing investigation, the cognizant privacy officer 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 cognizant HPSE or Regional Director 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. 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 6, 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.

(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.

(4) If notification is made, a copy of the notification must be sent to the DCAA privacy advisor.

7. INFORMATION REQUIREMENTS.

a. The annual Privacy Act report has been assigned Report Control Symbol DD-COMP(A)1379. Reporting requirements are prescribed and detailed in DoD 5400.11-R (reference b).

b. This instruction Adopts DD Form 2930, Privacy Impact Assessment (PIA), dated November 2008 and DPO Lost, Stolen, or Compromised Personally Identifiable Information Breach Report, dated October 2009

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

9. EFFECTIVE DATE. This instruction is effective immediately.

/s/
Patrick J. Fitzgerald
Director

Enclosures
1. References
2. Privacy Act Violations
3. DoD Privacy Impact Assessment (PIA) Format
4. Reporting Flowchart for Actual or Suspected PII Compromise
5. Report of Potentially Compromised Personally Identifiable Information (PII)
6. Risk Assessment Guide

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) Title 5, United States Code, Section 552a (http://privacy.defense.gov/files/pa1974.pdf)

(b) DoD 5400.11-R, DoD Privacy Program, May 14, 2007, (http://privacy.defense.gov/files/540011r.pdf)

(c) DCAAR 5410.8, DCAA Freedom of Information Act Program, May 17, 2000 (updated February 16, 2001) (available on the DCAA Intranet)

(d) 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 (http://www.whitehouse.gov/omb/memoranda/m03-22.html)

(e) DCAAR 8500.1, Information Assurance (IA) Program, September 24, 2009, (available on the DCAA Intranet)

(f) DoDI 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, February 12, 2009, www.dtic.mil/whs/directives/corres/pdf/540016p.pdf

(g) The Privacy Act: An Employee Guide to Privacy, March 7, 2012, (available on http://www.dcaa.mil/)

(h) Office of Management & Budget (OMB) Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007, (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf)

(i) DCAAP 8500.3, DCAA Computer Incident Response Plan, April 2009, (available on the DCAA Intranet)

ENCLOSURE 2

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 3

DOD PRIVACY IMPACT ASSESSMENT (PIA) FORMAT

Figure 1. DoD Privacy Impact Assessment (PIA) Format.

PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enter DoD Information System/Electronic Collection Name
Enter DoD Component Name

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

DD FORM 2930 NOV 2008 Page 1 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☐ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☐ **Yes, DITPR** Enter DITPR System Identification Number
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☐ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☐ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

DD FORM 2930 NOV 2008 Page 2 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

DD FORM 2930 NOV 2008 Page 3 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

- ☐ **Within the DoD Component.**
  - Specify.
- ☐ **Other DoD Components.**
  - Specify.
- ☐ **Other Federal Agencies.**
  - Specify.
- ☐ **State and Local Agencies.**
  - Specify.
- ☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)
  - Specify.
- ☐ **Other** (e.g., commercial providers, colleges).
  - Specify.

DD FORM 2930 NOV 2008 Page 4 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

DD FORM 2930 NOV 2008 Page 5 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

DD FORM 2930 NOV 2008 Page 6 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☐ Name	☐ Other Names Used	☐ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☐ Other ID Number
☐ Citizenship	☐ Legal Status	☐ Gender
☐ Race/Ethnicity	☐ Birth Date	☐ Place of Birth
☐ Personal Cell Telephone Number	☐ Home Telephone Number	☐ Personal Email Address
☐ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☐ Marital Status	☐ Biometrics	☐ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☐ Military Records
☐ Emergency Contact	☐ Education Information	☐ Other

If "Other," specify or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Describe here.

DD FORM 2930 NOV 2008 Page 7 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

(3) How will the information be collected? Indicate all that apply.

- ☐ **Paper Form**
- ☐ **Face-to-Face Contact**
- ☐ **Telephone Interview**
- ☐ **Fax**
- ☐ **Email**
- ☐ **Web Site**
- ☐ **Information Sharing - System to System**
- ☐ **Other**

If "Other," describe here.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Describe here.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Describe here.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

- ☐ **Yes**
- ☐ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

DD FORM 2930 NOV 2008

Page 8 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☐ **Users** ☐ **Developers** ☐ **System Administrators** ☐ **Contractors**

☐ **Other**

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☐ **Security Guards**	☐ **Cipher Locks**
☐ **Identification Badges**	☐ **Combination Locks**
☐ **Key Cards**	☐ **Closed Circuit TV (CCTV)**
☐ **Safes**	☐ **Other**

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

☐ **User Identification**	☐ **Biometrics**
☐ **Password**	☐ **Firewall**
☐ **Intrusion Detection System (IDS)**	☐ **Virtual Private Network (VPN)**
☐ **Encryption**	☐ **DoD Public Key Infrastructure Certificates**
☐ **External Certificate Authority (CA) Certificate**	☐ **Common Access Card (CAC)**

☐ **Other**

If "Other," specify here.

DD FORM 2930 NOV 2008 Page 9 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

(3) Administrative Controls. Indicate all that apply.

- ☐ **Periodic Security Audits**
- ☐ **Regular Monitoring of Users' Security Practices**
- ☐ **Methods to Ensure Only Authorized Personnel Access to PII**
- ☐ **Encryption of Backups Containing Sensitive Data**
- ☐ **Backups Secured Off-site**
- ☐ **Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☐ **Yes. Indicate the certification and accreditation status:**

☐ **Authorization to Operate (ATO)**	**Date Granted:**	
☐ **Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐ **Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐ **Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Describe here.

DD FORM 2930 NOV 2008 Page 10 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Describe here.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe here.

DD FORM 2930 NOV 2008 Page 11 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

DD FORM 2930 NOV 2008 Page 12 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Component Senior Information Assurance Officer Signature or Designee	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Component Privacy Officer Signature	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

DD FORM 2930 NOV 2008 Page 13 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

Component CIO Signature (Reviewing Official)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

DD FORM 2930 NOV 2008 Page 14 of 15

Figure 1. DoD Privacy Impact Assessment (PIA) Format, Continued

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

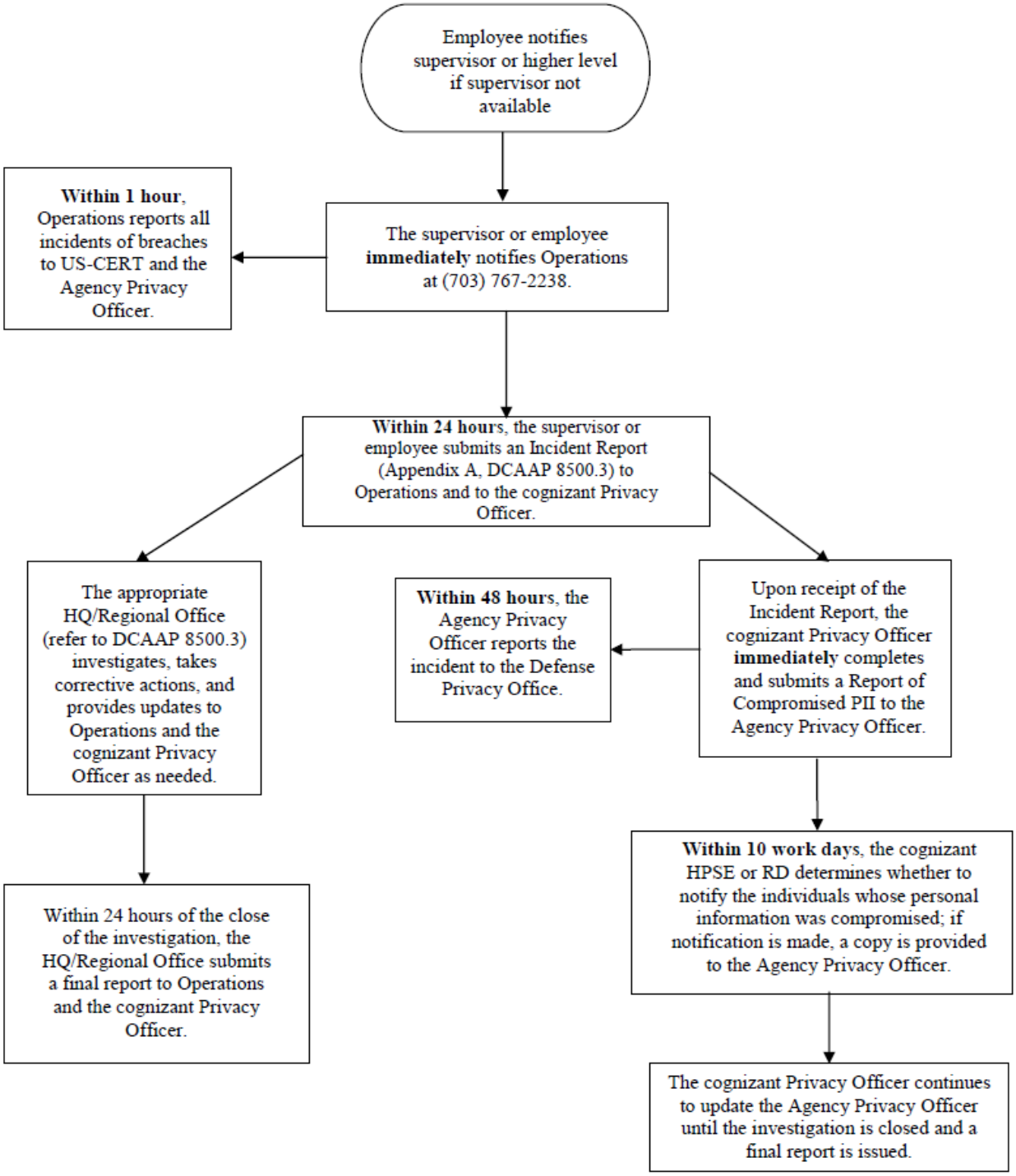
Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency 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. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.

ENCLOSURE 4

REPORTING FLOWCHART FOR ACTUAL OR SUSPECTED PII COMPROMISE

Figure 2. Reporting Flowchart for Actual or Suspected PII Compromise.



ENCLOSURE 5

REPORT OF POTENTIALLY COMPROMISED PERSONALLY IDENTIFIABLE INFORMATION (PII)

Figure 3. DPO Report.

INSTRUCTION FOR COMPLETING LOST, STOLEN, OR COMPROMISED PERSONALLY IDENTIFIABLE INFORMATION BREACH REPORT

Use this template to report and provide updates on the occurrence of lost, stolen, or compromised personally identifiable information submitted after October 2, 2009.
• Do not use acronyms when completing this template. • When events require an update to the original report due to significant changes, provide previous dates the report was submitted, any revisions, or additions to the original report in red text and note it as an updated report in item #3 of the revised report. • Submit this template and subsequent updates to dpo.correspondence@osd.mil.

1-7. Self explanatory.

8. Describe the breach. Summarize the facts of the breach, with clarity, in 150 words or less as you currently know them, including:

- facts and circumstances surrounding the loss, theft, or compromise;
- if the breach was internal, external, accidental, or intentional;
- type of incident and if the data was in a secure location (e.g., locked room, cabinet, etc.,);
- if any documents were posted to DoDs Internet or Intranet;
- if any documents were faxed inside or outside of DoD
- whether the breach was investigated, if the breach is isolated or a systematic problem, who conducted the investigation and any preliminary results available;
- whether the impacted individuals will be or were notified within 10 work days, or if necessary, action initiated to notify the Deputy Secretary of the inability to meet this notification requirement;
- any other pertinent information that you believe is relevant and pertinent.

9. Describe actions relevant to the incident. For example, actions taken to mitigate any harm that could result from the loss; remedial actions that have been, or will be taken to prevent similar incidents in the future, if the data was recovered, additional training conducted, policy or guidance issued.

10. Self explanatory

11. Provide the System of Records Notice(s) associated with the collection of the information lost, stolen or compromised *(Submission suspended until further notice).*

12. Self explanatory.

Figure 3. DPO Report, Continued

MEMORANDUM FOR DoD BREACH REPORTING

SUBJECT: Lost, Stolen, or Compromised Personally Identifiable Information Breach Report

1a. Date of Breach: **1b. Breach Discovery Date:**

2a. US-CERT Number: **2b Date Reported to US-CERT:**

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

3a. If no, what were the dates of the previous reports?
(Note: Report updates should be made in red text.)

4. DoD Component and organization involved:

Component Name	
Organization	
POC **Title/Organization**	
Telephone	
Email	

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

Name	
Address	
Title/Organization	
Telephone	
Email	

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

6a. Breakout number by category:

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

7. Did this incident involving one of the following:

(Select those that apply):

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

7a. If the incident involved equipment, what was lost, stolen or breached? How many pieces of equipment were involved in the incident? ☐ **N/A**

Figure 3. DPO Report, Continued

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

7b. How was the equipment protected? (Select all that apply):

Personally Owned	☐	**Password Protected**	☐
Encryption Software installed	☐	**PKI/CAC Enabled**	☐
Contractor Owned	☐	**Not protected**	☐
Government Owned	☐	Other (specify)	☐

7c. 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)	☐	☐

7d. Type of Personally Identifiable Information involved in the incident (Select all that apply):

Type of PII	Select all that apply	Type of PII	Select all that apply
Social Security Numbers (SSN)	☐	DOB	☐
Names	☐	PHI (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)

9. Describe actions taken in response to the breach. (150 words or less. Bulleted format is acceptable)

10. Potential impact of the breach (choose one from below)

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.

Figure 3. DPO Report, Continued

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.

Reference: DA&M Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", June 5, 2009

11. Associated System of Record Notice(s): *Submission suspended until further notice.*

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

Name	
Address	
Title/Organization	
Telephone	
Email	

ENCLOSURE 6

RISK ASSESSMENT GUIDE

Table 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 HPSE 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**	
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.**

No	Factor	Risk Determination	Comments
	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 Identity Theft Task Force found at http://www.idtheft.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.