DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

FEB 28 2013

MEMORANDUM FOR DLA EXECUTIVE BOARD

SUBJECT: Policies and Procedures When Personal Information is Lost, Stolen, or Compromised

As noted in my 7 June 2007 Memorandum on this topic, it is Department of Defense (DOD) policy[1] that the privacy of an individual is a personal right that shall be respected and protected. DOD's need to collect, maintain, use or disseminate personal information about individuals shall be balanced against the right of the individual to be protected against unwarranted invasions of their privacy. Accordingly, all DOD personnel, to include contractors, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, using or disseminating personal information[2] about an individual.

Further, whenever a DOD Component (e.g., the Defense Logistics Agency (DLA)) becomes aware that records containing personally identifiable information (PII), are lost, stolen or compromised (i.e., breach[3]), the potential exists that the records may be used for unlawful purposes such as identity theft, fraud, and stalking. The personal impact on the affected individuals may be severe if the records are misused. To assist the individual, and achieve effective breach management, DOD policy[4] requires that the Component use a "best judgment" standard to determine when to notify individuals of any loss, theft, or compromise. When using this standard the sensitivity of personal information is weighed against the likelihood of harm caused by the disclosure. This standard is discussed more fully in the attached.

DLA is implementing this best judgment standard for effective breach management by issuing the attached revised policies and procedures, which lists the actions that must be taken by DLA personnel and contractors in the event of any loss, theft, or compromise of PII. Please give the attached document wide dissemination within your organization.

(b)(6) - signature

FRED T. PRIBBLE
General Counsel

Attachment
a/s

---

[1] DoD Directive 5400.11, "Department of Defense Privacy Program," Sep. 1, 2011

[2] For definition of "personal information," also referred to as "personally identifiable information (PII)," see attachment – *Definitions*.

[3] For definition of "breach" see attachment – *Definitions*.

[4] Memorandum from Director, Administration and Management, and DoD Senior Official for Privacy to Component Privacy Officers, "Subject: Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations," Aug. 2, 2012

DEFENSE LOGISTICS AGENCY

Policies and Procedures when Personal Information is Lost, Stolen, or Compromised[1]

Version 2 – February 2013

[1] Attachment for Memorandum from DLA General Counsel to DLA Executive Board, "Subject: Policies and Procedures When Personal Information is Lost, Stolen, or Compromised," Feb. 28, 2013

Contents

1.0 PREFACE 3
Table 1. Record of Changes 3
2.0 PURPOSE 4
3.0 SCOPE 4
4.0 APPLICABILITY 4
5.0 DEFINITIONS 4
6.0 INCIDENT DETECTION AND REPORTING 6
7.0 INCIDENT RESPONSE TEAM (IRT) RESPONSIBILITIES 7
8.0 PHYSICAL VS. ELECTRONIC BREACH PROCESSING 8
9.0 PROCESS FOR "HIGH RISK" BREACHES 10
10.0 NOTIFICATION TO AFFECTED INDIVIDUALS 11
11.0 CONTRACTOR MAINTAINED PII 12
12.0 CLOSING AN INCIDENT WITH THE DLA NOSC / DLA CERT 13
13.0 RETENTION SCHEDULE FOR INCIDENT REPORTS 13
14.0 APPENDIX A – How to Categorize and Remediate Electronic PII Events 14
15.0 APPENDIX B – DPCLO Breach Report Template 20
16.0 APPENDIX C – Likelihood Determination Methodology 21
17.0 APPENDIX D – Assessing the Risk of Harm 26
18.0 APPENDIX E – Sample Notification Letter 28

1.0 PREFACE

On September 20, 2006, the Office of Management and Budget (OMB) issued a Memorandum to the Heads of the Departments and Agencies entitled "Recommendations for Identity Theft Related Data Breach Notification." OMB wrote, "Given the volume of personal information appropriately collected to carry out myriad government functions, it is almost inevitable that some agencies will, on occasion, lose control of such information." Agencies must be prepared for such losses and should respond accordingly to protect the individuals who might be affected.

The DoD Privacy Program regulation was updated Apr. 13, 2007 (72 FR 18758) to require DoD Components to "establish procedures to ensure that US Computer Emergency Response Team (CERT) reporting" of PII breaches is met. OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007, required agencies to develop and implement a notification policy for breach of PII. The Defense Logistics Agency (DLA) implemented the DoD and OMB requirements in a June 2007 General Counsel Memorandum – providing policies and procedures for when PII is lost stolen or compromised as an attachment.

OSD (Administration and Management) memorandum dated June 5, 2009, entitled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)" issued DoD-wide policy incorporating OMB Memorandum 07-16 requirements into the DoD Privacy Program (DoDD 5400.11 and DoD 5400.11-R). DLA updated the attachment to the June 2007 General Counsel Memorandum in March 2010 to address the changes from the June 5, 2009 OSD Memorandum.

OSD (Administration and Management) memorandum dated August 2, 2012, entitled, "Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations," altered DoD Privacy Program policy to incorporate OMB Memorandum 07-16, footnote 6 to use a "best judgment standard to develop and implement a breach notification policy." The below update to policies and procedures addresses the policy changes implemented with the August 2, 2012 OSD Memorandum. A summary of changes to the policies and procedures is in the table below.

Table 1. Record of Changes

Change Number	Date of Change	Section	Description of Change
Version 1.0	June 2007	Full document	Initial approved procedures
Version 1.1	March 2010	Full document	• Incorporated definitions and footnotes into procedures. • Added risk methodology, incident reporting format, and sample notification letter as appendices.
Version 2	February 2013	Full document	• Administrative updates to reflect organizational changes of DLA. • Assignment of low impact Technical

			Assessments from DLA CERT to PLFA Information Assurance Managers.
		Appendix A	• Addition of categorization methodology for electronic PII incidents. • Addition of Data Loss Prevention policies and procedures.

2.0 PURPOSE

The purpose of this document is to establish DLA's policies and procedures for responding to data breaches involving personal information / PII, should they occur within any of the DLA Components or in connection with work done by DLA contractors. It addresses the detection and reporting of such incidents, the assessment of their risk, and the appropriate notification.

3.0 SCOPE

These procedures provide responses to suspected or actual data breaches involving PII in the control of DLA or contractors who process, store, or possess DLA PII. It includes procedures for organizational actions in response to such events.

4.0 APPLICABILITY

4.1 These policies and procedures apply to any suspected or actual breach of personal information (PII) maintained by DLA or one of its contractors. In this policy, the term "maintain" includes the functions maintain, collect, use, and disseminate.

4.2 These procedures apply to the DLA Enterprise, and define the responsibilities associated with a breach for the following:

- DLA Computer Emergency Response Team (DLA CERT)
- Network Operations and Security Center (NOSC)
- Local Counsel
- DLA Privacy Officers and/or local Security Officers (when applicable)
- Information Assurance Managers (IAM) (when applicable)
- Local Field Activity DLA Office of Accountability point of contact (when applicable)
- All DLA personnel, contractors, and others who process, store, or possess personal information and/or personally identifiable information (PII) on behalf of DLA

5.0 DEFINITIONS

5.1 Breach: An actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected, *see* 32 CFR § 310.4(j)

5.2 Electronic media: Media that utilize electronics or electromechanical energy for the end user (audience) to access the content. This is in contrast to static media (mainly print media), which are most often created electronically, but don't require electronics to be accessed by the end user in the printed form. The primary electronic media sources familiar to the general public are better known as video recordings, audio recordings, multimedia presentations, slide presentations, CD-ROM and Online Content. Most new media are in the form of digital media. However, electronic media may be in either analog or digital format. Although the term is usually associated with content recorded on a storage medium, recordings are not required for live broadcasting and online networking. Example: Data on a CD stored electronically is electronic. If the data is written by a marker pen on the CD, it is physical.

5.3 High risk: Any Defense-wide, organizational (e.g., unit or office), or program or project level compilation of electronic records containing PII on 500 or more individuals stored on a single device or accessible through a single application or service, whether or not the compilation is subject to the Privacy Act.

- Any compilation of electronic records containing PII on less than 500 individuals identified by the Information or Data Owner as requiring additional protection measures.

- Individually identifiable medical or financial information.

- Law enforcement and other investigative reports containing PII.

Examples: Each event must be evaluated in the context of its specific facts, however a single unencrypted mobile computing or storage device containing PII on 500 or more individuals, even if the PII is distributed across multiple files or directories, is considered high risk PII. A counter example would be a DoD enclave of 500 or more users, with the PII for each individual user embedded in his/her individual whole-disk encrypted workstation, is not considered high risk PII. An unencrypted e-mail containing a scanned note from a physician regarding an employee's serious medical condition sent to individuals without a need to know is likely high risk PII.

5.4 Identity theft: Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

5.5 Incident Response Team (IRT): Local DLA Officials responsible for the investigation into and the reporting of the suspected incident. The IRT is made up of

the local IAM, the local Privacy Officer and/or local Security Officer (if applicable), a member of the local Counsel, and, if appropriate, the DLA Office of Accountability Field Officer. For physical incidents, the local IAM is not a member of the IRT.

5.6 Personal Information: Information about an individual maintained by an agency[2], including, but not limited to, education, financial transactions, medical history, and criminal or employment history and 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 an individual. Such information is also known as "personally identifiable information (PII)."

5.7 Physical media: Where the personal information and/or PII was in hardcopy, paper, or printed format.

5.8 Threat-source: Refers to whom the data was breached, e.g., federal employees, members of the military, contractors, the general public, or targeted hackers.

5.9 10-day notification period: If notification to the affected individual(s) is required (see process below), it must be made as soon as possible, but not later than 10 working days after the breach is discovered and the identities of the affected individuals ascertained.

- The 10-day period begins to run after DLA is able to determine the identities of at least some of the individuals whose records were lost, stolen, or compromised.

- If DLA is only able to identify some, but not all, of the affected individuals, then notification shall be given to those that can be identified with follow-up notifications made to those subsequently identified.

- If DLA cannot readily identify the affected individuals or will not be able to identify the individuals, then DLA shall provide a generalized notice to the potentially impacted population by whatever means DLA believes is most likely to reach the affected individuals, which could include posting notice to DLA website, social media, or news outlets.

6.0 INCIDENT DETECTION AND REPORTING

6.1 The DLA civilian employee, Service member, or contractor who discovers a suspected or actual breach of personally identifiable information (PII) will immediately call and report the discovery to the **DLA Network Operations and Security Center (NOSC)** at 1**-877-DLA-NEMO (1-877-352-6366)**.

[2] DLA is responsible for the information security of "information collected or maintained by or on behalf of an agency." A user independently choosing to store his PII where others may gain unauthorized access is not a collection or maintenance action "by or on behalf of an agency." Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3543(a)(2)(A).

6.2 If the DLA data loss prevention technology (DLP) identifies either a PII Incident (PI) or a PII Breach (PB), as determined by the criteria in Appendix A below, the DLP will forward the PI or PB details to the DLA NOSC so that the NOSC may begin to process it in accordance with the below procedures. Each PI or PB, upon detection and categorization by the DLP, will be reported by the DLA NOSC to US CERT as a suspected breach of PII.

6.3 The DLA NOSC will obtain as much information about the suspected or actual breach as possible, assign it a DLA NOSC Remedy Ticket Number, and determine if the incident involves physical records (paper) or electronic media records. DLP incidents elevated to the DLA NOSC in accordance with paragraph 6.2 will also be assigned a DLA NOSC Remedy Ticket Number.

6.4 The DLA NOSC will notify via email the DLA Computer Emergency Response Team (CERT), the local Information Assurance Manager (IAM), the local Privacy Officer, and the DLA Privacy Office (DG/DGA). The local Privacy Officer will notify the local Counsel of all suspected breaches.

6.5 The DLA NOSC will notify the US-CERT within the one-hour required timeframe. Initially, each breach will be reported by the DLA NOSC to US CERT as a suspected breach of PII.

6.6 During the course of a breach investigation, the DLA NOSC has the authority to direct tasks be accomplished by each DLA Component, as required, to complete an investigation in a timely manner.

7.0 INCIDENT RESPONSE TEAM (IRT) RESPONSIBILITIES

7.1 For all breaches reported to the DLA NOSC, within 24 hours of the discovery, the DLA Privacy Office (DG/DGA) will use the information provided in the DLA NOSC notification e-mail (see paragraph 6.4 above) to submit an Interim Incident Report, including the assigned DLA NOSC Remedy Ticket Number, to the Defense Privacy and Civil Liberties Office (DPCLO). The DLA Privacy Office will provide a copy of the Interim Incident Report e-mail to the IRT and the DLA CERT when it is sent to the DPCLO.

7.2 Within four business days of the suspected breach's discovery, using the process beginning at paragraph 8.0 below, the IRT must determine whether the incident involving PII reaches the threshold of a "high risk" breach. If a breach occurred, the 10-day notification clock started at the time DLA was able to identify the individuals whose PII was affected.

7.3 If the IRT determines it is both possible and necessary to provide notification to affected individuals, although the breach does not meet the criteria for being "high risk," the local Counsel will coordinate production of the notifications and provide them to the affected individuals within 10 business days of discovery of the breach of PII.

7.3.1. If a local Counsel intends to provide notification to affected individuals, he or she will send notice to the DLA Privacy Office (hq-privacy@dla.mil) at least one business day prior to providing the notice.

7.4 An investigation that follows standard DLA Office of Investigation / Army Regulation (AR) 15-6 procedures must be performed for all "high risk" breaches.

7.5 For breaches below the "high risk" threshold, the IRT will assess the incident to determine if there is a need for an investigation involving the DLA Office of Inspector General. If such an investigation is required, the IRT will notify the DLA Privacy Office and the investigation will follow standard DLA Office of Investigation / AR-15 procedures. The result of the investigation will be provided to the local Commander for disposition.

8.0 PHYSICAL VS. ELECTRONIC BREACH PROCESSING

8.1 If the suspected breach is **physical:**

8.1.1 And there are computer security implications (i.e., system access forms), within an hour of being informed, the DLA NOSC will alert the JTF-GNO and the local IT Chief in addition to those specified in paragraph 6.4 (above). Additionally, the DLA NOSC will provide an information copy to J-6 and DLA NOSC management. If there is no Privacy Officer at the Field Activity, then the DLA NOSC will contact the local Security Officer.

8.1.2 And there are no computer security implications, (e.g., medical or personnel paper records), within an hour of being informed, the DLA NOSC will alert J-6 and DLA NOSC management in addition to those specified in paragraph 6.4 (above). If there is no Privacy Officer at the Field Activity, then the DLA NOSC will contact the local Security Officer.

8.1.3 For all suspected physical breaches, the local Privacy Officer or the Security Officer will ensure the underlying cause that led to the breach has been contained via investigation, inquiry, or other actions taken to mitigate any harm that could result in accordance with DoD Privacy Program (32 CFR Part 310). At a minimum, all records containing PII must be physically secured by the IRT and reviewed for record retention compliance by the PLFA Records Officer.

8.2 If the suspected breach is **electronic**:

8.2.1 Within an hour of being informed, the DLA NOSC will alert the local IT Chief, and both J-6 and DLA NOSC management in addition to those specified in paragraph 6.4 (above).

8.2.2 If the DLA CERT determines that the technical aspects of the suspected breach appear routine, then the DLA CERT will send an email to the local Information Assurance Manager (IAM) to commence incident handling

procedures in accordance with established DoD and DLA Information Assurance policies and procedures – including CJCSM 6510.01B, "Cyber Incident Handling Program," (Jul. 10, 2012), DLA's Information Assurance Operational Controls One Book chapter, and the most current DLA's Incident Handling Guide, available on the DLA CERT webpage). The DLA CERT will provide a Technical Assessment based on the facts provided and assign a Likelihood Determination Level, as defined in Table 1-1 of Appendix C. The local IAM and the IRT will report using the existing NOSC Number and the IAM will ensure the underlying cause that led to the breach has been contained. The IAM will continue to report in accordance with established DLA procedures until the underlying cause that led to the breach situation (e.g., computer incident, theft, loss of material, etc.) has been resolved.

8.2.3 If the suspected breach has computer security implications or the DLA CERT determines it is complicated, in addition to the DLA CERT email to the local IAM described in 8.2.2 above, the DLA CERT will open a computer security incident, coordinate, and at its discretion take charge of, the incident investigation effort. The DLA CERT will provide a Technical Assessment based on the facts provided. The local IAM and the IRT will report using the existing NOSC Number, and the IAM will ensure the underlying cause that led to the breach has been contained. The IAM will continue to report in accordance with established DLA procedures until the underlying cause that led to the breach situation (e.g., computer incident, theft, loss of material, etc.) has been resolved.

8.3 If containment of the underlying cause requires disabling or disconnecting a MAC I or MAC II information system, the local IAM will contact the DLA Chief Information Officer (CIO) to obtain approval before proceeding. The DLA CIO may, as deemed necessary, consult with the local Commander and Information Owner prior to disabling or disconnecting an information system.

8.4 After obtaining the DLA CIO's approval, the local IAM will disable or disconnect the MAC I or MAC II information system and then notify the local Commander, Information Owner, and Counsel.

8.5 On or before the beginning of the fourth day following report of the breach, the local IAM will provide to the local Privacy Officer and to the DLA CERT the facts and type of PII involved, actions taken in response to the breach, number and type of people whose PII was involved (e.g., Military, DoD Civilian, Members of the Public, Dependents, etc.), and the number of people who were exposed to/saw/received the PII.

8.5.1 The local IAM will provide DLA CERT with forensic information the DLA CERT deems necessary to: (1) make a technical assessment as to the likelihood that the PII has been accessed; by how many and if possible whom; and since when; and (2) the technical and data details pertaining to the

incident, e.g., the type of PII involved, actions taken in response to the incident, number of individuals whose PII was exposed.

8.5.2 If the data provided by the IAM does not validate the Technical Assessment, the DLA CERT will review the Technical Assessment before the end of the 4th day and determine the Technical Assessment. The DLA CERT is the final authority in determining when adequate forensic information has been provided by the IAM to produce an accurate Technical Assessment.

8.6 If the incident is routine as defined by 8.2.2 (see above), the local IAM will provide the DLA Privacy Office (DGA) with the Technical Assessment by the end of the fourth day. Technical Assessment information must be e-mailed to hq-privacy@dla.mil.

8.7 If the incident is complicated as defined by 8.2.3 (see above), the DLA CERT will either provide the DLA Privacy Office (DGA) with the Technical Assessment, or a request for an extension by the end of the fourth day. Technical Assessment information and extension requests must be e-mailed to hq-privacy@dla.mil. An extension may be granted based on the facts of the incident and its likely impact level. NOTE: High Impact incidents may not be granted an extension.

9.0 PROCESS FOR "HIGH RISK" BREACHES

9.1 The local Counsel will immediately notify the DLA General Counsel and the DLA Privacy Office (hq-privacy@dla.mil) of a "High Risk" breach.

9.2 The DLA Privacy Office will provide a report of the "high risk" incident to (1) the DLA General Counsel, and (2) the Defense Privacy and Civil Liberties Office by the end of the second day after the discovery of the "high risk" breach of PII.

9.2.1 The reports in 9.2 (above) will be based on information from the Interim Incident Report, and any other additional details, provided by the DLA CERT or IRT.

9.3 Within five business days of discovery of the breach, the IRT will determine whether the local Field Activity will provide notice to all affected individuals within the mandated 10-business days of discovering the breach.

9.4 When making the notification determination, the IRT will take the Likelihood Determination Level provided by the DLA CERT and assess the likely Magnitude of Impact caused by the breached information to compute the Risk-Level occurring. The IRT will consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach. *The IRT will bear in mind that notification when there is little or no risk of harm might create unnecessary concern and confusion.* There are five factors that must be considered to assess the risk of harm (See Appendix D). The IRT must document its rationale and the resulting "Risk-Level" determination (see Table 1-3 of Appendix C).

9.5 If the IRT cannot reach a Likelihood Determination Level, then the decision will be elevated, through the DLA Privacy Office, to DLA General Counsel or his designee.

9.6 If the IRT determines that notification is required and it will not be possible to provide notification to the affected individuals within 10 business days, the local Counsel will prepare a memorandum for the Deputy Secretary of Defense for signature by the Director of DLA providing a brief summary of what occurred, why notification was not provided within the required 10 business days, and what actions are being taken, highlighting the exact date notifications will commence and their anticipated completion date.

9.6.1 This "deadline" memorandum must be transmitted by the Field Activity Commander to the Director of DLA, with a courtesy copy to the General Counsel.

9.6.2 This memorandum shall be transmitted via the Deputy Under Secretary of Defense, Acquisition, Logistics and Technology through the Under Secretary of Defense for Personnel and Readiness with a copy to the Defense Privacy and Civil Liberties Office.

9.7 The DLA General Counsel's Office, in consultation with the DLA CIO and the Field Activity involved will make a determination of whether it will be (a) necessary and (b) possible for DLA to provide the required notice to all affected individuals within 10 business days. This notification determination shall be made within two business days of receiving the "high risk" determination from the IRT described in paragraph 9.2 (above).

9.8 The General Counsel will either prepare the required notifications to the affected individuals with the assistance of the DLA CIO and the Field Activity involved or delegate this preparation to the local Counsel so that notification is provided within the required 10 business days.

9.9 Where DLA is providing data services for another DoD Component or Federal agency, the local Counsel will immediately notify the other agency of the data breach and DLA's response plans.

9.10 If the breach involves Government credit card information, DLA shall notify the issuing bank at the same time affected individuals are notified.

9.11 In situations involving questions of interpretation, the DLA CERT will have final authority in making a determination whether access has occurred.

10.0 NOTIFICATION TO AFFECTED INDIVIDUALS

10.1 Letters are the recommended method for notification involving breaches of personal information/PII of members of the general public, although digitally signed e-mail notification is permissible. A sample notification letter is at Appendix E.

10.2 Notifications to affected individuals shall contain, at a minimum, the following information:

10.2.1 The specific data was involved. It is insufficient to simply state that personal information has been lost, stolen, or compromised. Where names, social security numbers, and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.

10.2.2 The facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so that the individual clearly understands how the compromise occurred.

10.2.3 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.

10.2.4 A description of what DLA is doing to investigate the breach, mitigate losses, and protect against further breaches.

10.2.5 The protective actions DLA is taking or the individual can take to mitigate against potential future harm.

10.2.6 Steps that individuals should take to protect themselves from harm, such as the risk of identity theft, including the steps identified on the Federal Trade Commission's website, http://www.ftc.gov/bcp/edu/microsites/idtheft/. The site provides valuable information as to what steps individuals can take to protect themselves if their identities potentially have been or are stolen.

10.2.7 Contact procedures for questions or additional information, including a telephone number, email address, website, and/or postal address. The point of contact must be someone knowledgeable about the specifics of the breach and understand the steps individuals may take to protect themselves from the risk of identity theft. The Privacy Act Officer or Public Affairs Officer for the Field Activity where the breach occurs will often be the best suited to handle this activity. The phone number must be either direct or toll-free.

11.0 CONTRACTOR MAINTAINED PII

11.1 DLA Procurement Policy Letter (PROCLTR) 2012-05, "Privacy Act Requirements," (Oct. 31, 2011), provides "that there are mandatory clauses and requirements which must be included in any contract where the contractor will collect, maintain, use, disseminate, or destroy" personal information.

11.2 When personal information is maintained by a DoD contractor on behalf of DLA, the contractor shall immediately notify both the DLA NOSC and the DLA Contracting Officer responsible for the contract when it suspects that personal information has been lost, stolen, or compromised.

11.3 The DLA Contracting Officer responsible for the contract shall determine, in consultation with the DLA Privacy Office, whether DLA or the contractor shall make the required notification.

11.4 If the contractor is to notify the impacted population, it shall submit the notification letters to DLA General Counsel for review and approval. DLA shall coordinate with the contractor to ensure that the letters are timely and meet the requirements of these policies and procedures.

12.0 CLOSING AN INCIDENT WITH THE DLA NOSC / DLA CERT

12.1 The DLA Privacy Office (DG/DGA) is the only entity that may close an incident that was reported to the DLA NOSC as a suspected or actual breach.

12.1.1 Authority to close incidents elevated to the DLA NOSC from the DLP technology may be delegated to the local Privacy Officer.

12.2 The DLA Privacy Office (DG/DGA) will receive (at hq-privacy@dla.mil) a draft Final Incident report from the local IAM/Privacy Officer by the end of the 10th business day OR will have received a request for an extension from the local IAM or Privacy Officer (in case of a complicated incident). An extension may be granted based on the facts of the incident and its likely impact level. NOTE: High Impact incidents may not be granted an extension. .

12.3 The DLA Privacy Office (DGA) will submit the Final Incident Report to the Defense Privacy and Civil Liberties Office.

12.4 DLA Privacy Office will send a copy of the Final Incident Report to the DLA NOSC and DLA CERT to close the incident. The DLA NOSC will notify US CERT of the final disposition of the incident.

13.0 RETENTION SCHEDULE FOR INCIDENT REPORTS

Incident response reports (Appendix A) for breaches will be maintained pursuant to DLA Records Retention Schedule, 284.82 Incident (Compromise) Files -- Reports of compromises, involving personnel, cryptologics and physical insecurities of COMSEC material. (Destroy closed incident file after 2 years.) N1-361-91-1

14.0 APPENDIX A – How to Categorize and Remediate Electronic PII Events

Table 1. PII Event Category

PII Event Type	Nature of Event	
	Type I	*Type II*
Unauthorized Access (A)	A1	A2
Unauthorized Disclosure (D)	D1	D2
Unauthorized Modification (M)	M1	M2
Misuse (U)	U1	U2
Mishandle (H)	H1	H2
Not a PII Incident (NPI)	NPI	

Type I	An action demonstrating "a lack of attention, care or concern" for safeguarding PII in accordance with DLA or DoD requirements (Example – A user places a folder containing an unencrypted spreadsheet with 100 DLA employees' full names, SSNs, and dates of birth, on a DLA share drive.)
Type II	An action demonstrating a prudent and reasonable effort to comply with DoD and DLA requirements for safeguarding PII (Example – A user placing a single unencrypted document with only a few DLA employees' full names and home phone numbers on a DLA internal system in a folder with restrictive access controls. For additional clarification *see* "Policy Violation (PV)" below.)

Table 2. Quick-Chart: PII Remediation Category by PII Event Category [3]

	PII Event Category				
	NPI	H2	A2 & H1	U1/U2 & D1/D2	A1 & M1/M2
PII Remediation Category	**NPI**	**PV**	**PI**	**PI/PB** [4,5]	**PB**

[3] NOTE: A PII event may fit into more than a single "PII Event Category," e.g., a file on a share drive with division level access controls where the division has hundreds of employees may fit into both the H2 and D2 categories. As per NIST guidance regarding categorization of security incidents involving multiple vectors, a PII event involving multiple vectors should be remediated in the PII Event Category with the higher remediation requirements, e.g., in our example it would be the D2 category.

[4] U Event Type PII Remediation Category dependent on outcome of technical and possibly other investigations.

Table 3. PII Remediation Category Description and Remediation Requirements [6]

PII Remediation Category	Description	Remediation Management Required
Not a PII Incident (**NPI**)	An employee, who sends his own, unencrypted PII from his DLA e-mail account to his home e-mail, while not a good security practice, is not a PII incident as the employee may authorize the release of his own PII in any manner he chooses. An employee storing her own PII in an unencrypted manner on a DLA share drive, while a bad security practice would be permitted if technology could effectively differentiate between whether the PII belongs to the employee storing it on the share drive or not. However, with current DLP, it is not possible to determine if the PII detected belongs to the owner of the file who placed it on the share drive and that is why any PII found on a share drive will be treated at the **Policy Violation** (PV) level or higher.	None required.
Policy Violation (**PV**)	PII on a DLA internal system with restrictive access controls, e.g., PII on a DLA organizational share drive where access controls permit access	DLA Data Loss Prevention (DLP)[7] events meeting criteria for **Policy Violations** are remediated per the following process, and do not require escalation to

[5] D Event Type PII Remediation Category dependent on outcome of technical investigation. Factors include, but are not limited to, whether transmission is internal versus external and whether individuals receiving PII had appropriate authorization.

[6] OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," (May 22, 2007), Footnote 6 requires agencies to use a "best judgment standard to develop and implement a breach notification policy" when determining which incidents must be reported to US-CERT. This table establishes DLA's best judgment standard for events detected pursuant to Data Loss Prevention (DLP) scanning and evaluates how the sensitivity of the "personally identifiable information, can be determined in context" of its information technology environment.

[7] DLA uses a commercial-off-the-shelf (COTS) Data Loss Prevention (DLP) product that satisfies the requirements of an "*effective data loss prevention (DLP) strategy includ[ing] data inventory and classification; data metric collection; policy development for data creation, use, storage, transmission, and disposal; and tools to monitor data at rest, in use, and in transit;"* as set forth in the National Institute of Standards and Technology (NIST) Special Publication 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," (December 2010) on page D-8.

PII Remediation Category	Description	Remediation Management Required
	to only a limited number of DLA personnel such as administrative assistants, current team members, or other members of a cognizable group within a DLA organization. The number of personnel with access to the PII is typically less than 30 DLA users, although contributing factors such as clearance and responsibility of the users along with sensitivity of the data can result in increases or decreases to this number based on an assessment of these contributing factors. In such a situation, a Policy Violation (PV) has occurred. **NOTE**: To be a PV, the DLA organizational share drive must not have global access permissions where anyone who accesses the share drive would have access to the PII.	the DLA NOSC or CERT. First determine if the file containing the PII has a named DLA user as owner and not the "Administrator," or "System" account – either of which indicates an "ownerless" file under Windows File Management. If the file has either the "Administrator" or "System" owner, "move the file to secure" and leave a marker in the directory informing users that this file contained PII and has been quarantined. If the file has a named DLA user as owner, and it has not been modified in the past 2 years, "move the file to secure" and leave a marker in the directory informing that user that this file contained PII and has been quarantined. Access for named users will be restored with a request from their supervisor authorizing their access. When returned, the user should be informed of the requirement to password protect or encrypt the file. If the file has a named DLA user as owner and it has been modified in the past 2 years, the DLP re-mediator will flag the event for the file as containing PII using the DLP tool. These events will be tracked and reported as part of the overall DLP scanning program status as the Privacy Act requires audit and accountability.
PII Incident (**PI**)	PII stored on DLA internal system that does not utilize access controls (or only uses generic domain access controls, e.g., access controls limited to all USE4 Users) or PII transmitted across public switches to other Federal agencies without using encryption. Both incidents will require investigation to determine if a PII Breach (PB) has occurred or whether it remains a PII	Events meeting criteria for **PII Incidents** will be managed in accordance with the "DLA Policies and Procedures when Personal Information is Lost, Stolen, or Compromised," starting at paragraph 6 in the above document. Such events will be treated as a suspected breach of PII until the investigative process described in paragraph 8.2 and forward in the above document determines otherwise and will

PII Remediation Category	Description	Remediation Management Required
	Incident (PI).	be escalated to the DLA NOSC for reporting, tracking, DLA CERT investigation, and remediation. US CERT notification will be required. Employee discipline or contractual actions may be required and proper chain of evidence and incident tracking is required. NOTE: If DLA DLP later determines the event does not meet PII Breach criteria, then the DLP scanning program may record the event as a PII Incident (if appropriate) and US CERT notification may be canceled.
PII Breach (**PB**)	DLA PII stored or transmitted on/to an external system that does not have DoD-level security controls. Some examples include, but are not limited to, sending unencrypted e-mail containing PII to another Federal agency. Another example would be posting unencrypted documents containing PII on the Internet. A "PII Incident" becomes a "PII Breach" when the loss of either the security, integrity, or both, of the PII "could result in substantial harm, embarrassment, inconvenience, or unfairness to [the] individual on whom the information is maintained."	Events meeting criteria for **PII Breaches** will be managed in accordance with standard "DLA Policies and Procedures when Personal Information is Lost, Stolen, or Compromised," starting at paragraph 6 in the above document and will be escalated to the DLA NOSC for reporting and tracking and to the DLA CERT for investigation and remediation. US CERT notification will be required. Employee discipline or contractual actions may be necessary and proper chain of evidence and incident tracking is required.

Table 4. Definitions

TERM	ACRONYM	DEFINITION
Unauthorized Access	A	The act of a user or system gaining access to PII without authorization[8] (Example - An unauthorized user stumbling upon PII during their standard course of duty due to the improper application of access control lists (ACL's) for a directory.)
Unauthorized Disclosure	D	The act of a user or system providing, releasing, or making available, PII without appropriate authorization. (Example - An email containing PII is sent to unauthorized individuals.)
Unauthorized Modification	M	The act of a user or system changing PII without appropriate authorization or audit controls (Example - An individual makes unauthorized edits to the contents of a file containing PII.)
Misuse	U	The act of a user or system utilizing PII in a manner other than for which it was originally intended and/or authorized. (Example - Using PII originally collected under a published Privacy Act System of Records Notice that allows for the PII to be used for benefits purposes to be used instead to perform marketing, or vice versa.)
Mishandle	H	The act of a system or user improperly storing information (Example - PII stored in a location without an approved Privacy Impact Assessment or in an authorized location but the PII lacks required security controls.)
Not a PII Incident	NPI[9]	Events may be demoted to this event type, in accordance with the DLA DLP CONOPS[10], following review of the technical, administrative, and physical safeguards surrounding the event. This event type is intended primarily for situations where an employee sends his own unencrypted PII from his DLA e-mail account to his home e-mail. While such an event involves poor security practices by the employee, the employee may choose to disclose his PII in this manner and the manner of disclosure is not the responsibility of the agency.

[8] Authorization may be effected via DD Form 2875, "System Authorization Access Request (SAAR)," pursuant to 5 U.S.C. § 552a (b), or through another documented assignment of access by the responsible official or system manager.

[9] This definition applies to the use of NPI in Table 1. The remediation category description in Table 3 expands on this definition.

[10] DLA Data Loss Prevention Concept of Operations (on eWorkplace)

TERM	ACRONYM	DEFINITION
Access		The ability and means to communicate with (i.e., input to or receive output from), or otherwise make use of any information, resource, or component in an information system. Note: An individual does not have "access" if the proper authority or "administrative, technical, and physical safeguards"[11] prevents him/her from obtaining knowledge or having an opportunity to alter information, material, resources, or components.
DLA Internal System		A DoD Information System within the Enterprise Telecommunications Network under the purview of the DLA Designated Approving Authority.[12]

[11] 5 U.S.C. § 552a (e)(10): "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

[12] Definition provided by DLA NOSC.

15.0 APPENDIX B – DPCLO Breach Report Template

DPCLO Breach Report Template in Microsoft Excel Format

Breach Report Template.xlsx

16.0 APPENDIX C – Likelihood Determination Methodology

Based on NIST Special Publication 800-30

1. Likelihood Determination (Step 1):

a. To derive an overall likelihood rating that indicates the probability that a potential breach / vulnerability may be exercised within the construct of the associated threat environment; the following governing factors must be considered:
   - Threat-source motivation and capability
   - Existence and effectiveness of current controls.

b. The likelihood that a potential breach/vulnerability could be exercised by a given threat-source can be described as high, medium, low, or very low. Table 1-1 below describes these four likelihood levels.

c. Likelihood Determination Output —Likelihood rating (High, Medium, Low, Very Low)

Table 1-1. Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the breach/vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the breach/vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the breach/vulnerability from being exercised.
Very Low	The threat-source has been all but eliminated as having either motivation or capability either through forensics or through direct query.

2. Impact Analysis (Step 2):

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

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

c. If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and

confidentiality. Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners, in consultation with the local Counsel's Office, are responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s) and consult with the local Counsel's Office.

d. Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

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

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

    iii. *Loss of Confidentiality.* System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data or PII. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

e. Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts. Because of the generic nature of this discussion, this guide designates and describes only the qualitative categories—high, medium, and low impact (see Table 1.2).

f. Quantitative versus Qualitative Assessment

    i. In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

ii. The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to—

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

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

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

g. Output from Impact Analysis—Magnitude of impact (High, Medium, or Low).

Table 1-2. Magnitude of Impact Definitions

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

3. Risk Determination (Step 3)

a. The purpose of this step is to assess the level of risk to the IT system containing the Personally Identifiable Information (PII). The determination of risk for a particular threat/breach/vulnerability pair can be expressed as a function of—

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

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

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

b. To measure risk, a risk scale and a risk-level matrix must be developed. Section 3.1 presents a standard risk-level matrix; paragraph c. below describes the resulting risk levels.

c. Risk-Level Matrix.

i. The final determination of risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 1.3 below shows how the overall risk ratings will be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 4 x 3 matrix of threat likelihood (High, Medium, Low, and Very Low) and threat impact (High, Medium, and Low).

ii. The matrix in Table 1-3 shows how the overall risk levels of High, Medium, Low, and Very Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example,

1) The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low, 0.01 for Very Low. *If the level indicated on certain items is so low as to be deemed to be "negligible" or non-significant (value is <1 on risk scale of 1 to 100), one may wish to hold these aside in a separate bucket in lieu of forwarding for management action. This will make sure that they are not overlooked when conducting the next periodic risk assessment. It also establishes a complete record of all risks identified in the analysis. These risks may move to a new risk-level on a reassessment due to a change in threat likelihood and/or impact and that is why it is critical that their identification not be lost in the exercise.*
2) The values assigned the impact levels are 100 for High, 50 for Medium, and 10 for Low.

Table 1-3. Risk-Level Matrix

Threat Likelihood	**Impact**		
	Low (10)	**Medium (50)**	**High (100)**
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10
Very Low (0.01)	**Very Low** 10 X 0.01 = 0.1	**Very Low** 50 X 0.01 = 0.5	**Very Low** 100 X 0.01 = 1

Risk-Level: **High** (>50 to 100); **Medium** (>10 to 50); **Low** (1 to 10); **Very Low** (<1)

d. Description of Risk-Level. Table 1-4 describes the risk levels shown in Table 1-3. This risk scale, with its ratings of High, Medium, Low, and Very Low represents the degree or level of risk to which an IT system, facility, or procedure containing PII might be exposed

if a given breach/vulnerability were exercised. The risk-level also presents actions that senior management, the mission owners, must take for each risk-level.

e. Output from Step 3—Risk-level (High, Medium, Low, Very Low)

Table 1-4. Risk-Level And Necessary Actions

Risk-Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a need to provide notification to affected individuals, i.e., this PII breach requires notification under the 10-day rule.
Medium	If an observation is rated as medium risk, there may be a need to provide notification to affected individuals. The local Counsel's Office must contact DLA GC to discuss the results of this risk assessment and what next steps should be taken.
Low & Very Low	If an observation is described as low or very low risk, there is no need to provide notification to affected individuals. The likely harm to the individuals associated with this breach/vulnerability are so low that to notify them will not be a benefit to them and may result in falsely raising an alarm when any risks present are exceedingly low.

17.0 APPENDIX D – Assessing the Risk of Harm

FIVE FACTORS TO CONSIDER WHEN ASSESSING THE LIKELY RISK OF 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 level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.* It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context. *For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher risk of harm, whereas a database of names of subscribers to agency media alerts may pose a lower risk of harm.* In assessing the levels of risk of harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

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

3. Likelihood the Information is Accessible and Usable. Upon learning of a breach, agencies should assess the likelihood personally identifiable information (PII) will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the agency's decision to provide notification.

a. The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals, however, depending upon a number of physical, technological, and procedural safeguards employed by the agency. 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 NIST.

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

4. Likelihood the Breach May Lead to Harm.

a. *Broad Reach of Potential Harm.* Section 5 U.S.C. § 552a(e)(10) of the Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 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 valuable for committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other PII, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients patients at a clinic for treatment of a contagious disease. *In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the Identity Theft Task Force "Recommendations for Identity Theft Related Data Breach Notification"* (www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

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. *For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.* Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

18.0 APPENDIX E – Sample Notification Letter

DoD 5400.11-R, DoD Privacy Program

Dear Mr. John Doe:

On January 1, 2010, a DoD laptop computer was stolen from the parked car of a DoD employee in Washington, DC after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program. The compromised information is the name, social security number, residential address, date of birth, office and home email address, office, and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities, who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission (FTC) at its Web site at http://www.consumer.gov/articles/1016-recovering-identity-theft. The FTC urges that you immediately place an initial fraud alert on your credit file. The Fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The Department of Defense takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you. Should you have any questions, please call _____.

Sincerely,

Signature Block
(Directorate level or higher)