NATIONAL GUARD BUREAU
1636 DEFENSE PENTAGON
WASHINGTON, DC 20301-1636

National Guard Bureau
Arlington, VA 22202-3231
28 September 2010

NGB Memorandum 380-16/33-361

Information Security

PERSONALLY IDENTIFIABLE INFORMATION (PII) INCIDENT RESPONSE HANDLING

Summary. This memorandum establishes policy and provides guidance for coordination of the response to incidents involving breaches of Personally Identifiable Information (PII) in the National Capitol Region (NCR).

History. This is a new National Guard Bureau (NGB) Memorandum.

Applicability. This memorandum is applicable to all elements of the NGB including but not limited to, the Army and Air National Guard Directorates and all other NGB entities.

Proponent. The proponent for this memorandum is the NGB Office of the Chief Counsel's Office of Information and Privacy (NGB-JA-OIP).

Distribution. All elements of the NGB.

1. **Policy.**

a. The NGB/JA-OIP has oversight and responsibility to ensure all incidents involving the suspected or confirmed loss, theft, or compromises of PII are properly handled in accordance with established laws and policies.

b. Any individual discovering a suspected or confirmed PII Incident will immediately report the incident to NGB/JA-OIP (Privacy@ng.army.mil). NGB/JA-OIP will contact the appropriate directorate/division within the area where the incident occurred to take action in responding to the incident.

c. There will be a PII Core Management Group (CMG) (Encl 1) led by NGB/JA-OIP. Members of the PII CMG will meet quarterly to review all incidents reported by the states and make recommendations on future preventative actions and policies to improve protection of PII and incident reporting. Members of the PII CMG will meet within 48 hours of a PII breach within the NCR where the overall risk determination on the incident is "medium" or "high" based on the DoD Risk Assessment Model (Encl 5). This formulated team will be referred to as the PII Incident Response Team (IRT) (Encl 2).

2. **Responsibilities.**

a. The NGB Joint Staff (JS), Air, and Army Directors are responsible for appointing members to serve on the PII CMG and will provide those names to NGB/JA-OIP annually.

b. Designated members will follow the responsibilities outlined in Encl A and B.

c. The PII CMG expertise may also be called upon to assist in response to PII Breaches within the states.

3. **Exceptions.** Exceptions to this policy may only be granted by the CNGB. Any questions regarding this policy should be directed to Ms. Jennifer Nikolaisen, GS-14, Chief Privacy Officer, (703) 607-3195 or Privacy@ng.army.mil.

CRAIG R. MCKINLEY
General, USAF
Chief, National Guard Bureau

9 Encls
1. NGB PII CMG Composition/Responsibilities
2. NGB PII IRT Composition/Responsibilities
3. PII Breach Reporting Flow Chart
4. DoD PII Breach Report Template
5. DoD Risk Assessment Model
6. Risk of Harm Considerations
7. Breach Notification Considerations
8. References
9. Definitions

ENCLOSURE 1

NGB PII CORE MANAGEMENT GROUP (CMG) COMPOSITION/RESPONSIBILITIES

1. The PII CMG will be chaired by the NGB-JA-OIP. The CMG will meet quarterly to conduct a review all PII incidents reported throughout the National Guard (NG). The CMG will be responsible for seeking ways to remedy trends that may occur within specific functional areas and collaborating on ways to improve the protection of PII and PII Breach handling throughout the NG.

2. The members of the PII CMG will include, at a minimum:

- The NGB Privacy Officer (NGB-JA-OIP)
- Attorney(s) from Chief Counsel (JA)
- Representative(s) from Public Affairs (PA) Office
- Representative(s) from Legislative Liaison (LL) Office
- Representative(s) from Inspector General (IG) Office
- Representative(s) from Operational Contracting (AQ)
- Representative(s) from Directorate of Management (DM)
- Representative(s) from ANG, ARNG, and NGB Joint Staff (JS)

Manpower/Personnel Directorates (A1/G1/J1)

- Representative(s) from ANG, ARNG, and NGB JS Communications Directorates

(A6/G6/J6)

- Representative(s) from the respective ANG, ARNG, and NGB JS Intelligence

Directorates (A2/ARO-I/J2)

- Other advisory personnel as deemed necessary by the Directors

3. Each member of the PII CMG will be responsible for:

a. Providing advice and recommendations on improvement of policies and procedures on protecting PII and responding to PII incidents within their respective directorates and supporting field activities,

b. Design and issuance of supplemental guidance to field activities on PII breach trends occurring within their field activities as needed, and

c. Serving as members of the PII IRT on "High" or "Medium" impact PII Breaches within their respective ARNG, ANG, and NGB JS Directorates.

4. The NGB-JA-OIP will schedule all quarterly meetings and provide a summary of the meeting and quarterly PII Breaches within the National Guard to the PII CMG members.

ENCLOSURE 2

NGB PII INCIDENT RESPONSE TEAM (IRT) COMPOSITION/RESPONSIBILITIES

1. The PII IRT composition will vary depending on whether the incident occurred on the ARNG Staff, ANG Staff, or NGB JS.

2. When an incident occurs, the PII IRT will be chaired by the designee appointed by the Director of the ARNG Staff, ANG Staff, or NGB JS (depending on which staff the incident occurred). The members of the PII IRT will include, at a minimum:

- NGB Privacy Officer (NGB-JA-OIP)
- Attorney(s) from Chief Counsel (JA)
- Representative(s) from Public Affairs (PA) Office
- Representative(s) from Legislative Liaison (LL) Office
- Representative(s) from Inspector General (IG) Office
- Representative(s) from Operational Contracting (AQ)
- Representative(s) from Directorate of Management (DM)
- Representative(s) from the respective ANG, ARNG, and NGB JS

Manpower/Personnel (A1/G1/J1) Directorate where the incident occurred

- Representative(s) from the respective ANG, ARNG, and NGB JS Intelligence

(A2/ARO-I/J2) Directorate where the incident occurred

- Representative(s) from the respective ANG, ARNG, and NGB JS

Communications (A6/G6/J6) Directorate where the incident occurred

- The Designated Accreditation Authority (DAA) or his/her representative when an

information system they have accredited is involved in a breach

- The Information System Owner (ISO) when their system is involved in a breach

3. Responsibilities of the PII IRT:

a. The PII IRT Chairman will:

(1) Lead in the development of a mitigation strategy action plan in response to the PII Breach by serving as the Incident Response Commander and directing members of the PII IRT on actions needed to develop and execute action plans in response to the PII Breach, and,

(2) Apprise senior leadership on incident response handling as needed.

b. The NGB-JA-OIP will:

(1) Schedule convening of PII IRT meetings when required,

(2) Provide advice to IRT on mitigation strategies, policies, and procedures in response to PII Breaches,

(3) Maintain an incident file on each PII breach to include after-actions reports and other relevant records pertaining to incident, and,

(4) Monitor reported PII incidents involving computer assets to ensure they have been concurrently reported to the CND Team.

c. The NGB-JA will:

(1) Provide legal support and guidance in responding to PII, and

(2) Assist in guidance on disciplinary actions when required to include sanctions against contractors when necessary.

d. The NGB PA office will:

(1) Ensure notification to other public affairs offices (DoD, AF, AR) with regards to suspected or confirmed PII breaches is made when appropriate,

(2) Respond to media inquiries and interview requests regarding PII breaches, and,

(3) Develop and issue press releases and website notifications when appropriate.

e. The NGB LL office will inform members of Congress, as appropriate, regarding a PII breach and respond to any Congressional inquiries/committees on breaches.

f. The IG office will:

(1) Monitor and provide guidance regarding implementation and adherence to policies and procedures, and

(2) Inspect, investigate, and perform inquiries on PII breaches when necessary.

g. The DM office will:

(1) Assist in determining whether reporting to AF/AR and/or civilian law enforcement agencies and make those reporting when necessary,

(2) Coordinate on security protection measures as required in response to a PII breach, and,

(3) Restore security measures for protecting information if needed (e.g. replacement or installation of locks, ensuring that all file areas are accounted for).

h. The AQ Division will:

(1) Assist in evaluation and execution of contracts when outsourcing is needed to cover services in response to PII breach such as call centers, mailings, staffing, and security measures,

(2) Provide a copy of the contract to NGB-JA and NGB-JA-OIP if the breach was caused by a contractor, and,

(3) Work with NGB-JA in administration of contractor sanctions when necessary.

i. The Personnel Directorate for ANG, ARNG, or NGB JS will:

(1) Provide rules and consequences policy for mishandling of PII,

(2) Assist in the timely identification of contact information for individuals affected by PII breach using available systems under DoD's control,

(3) Review the list of individuals being notified against record of deceased within personnel databases to ensure families are not inadvertently notified whenever possible, and

(4) Provide labor/relations advice and guidance regarding corrective actions for individual(s) that caused PII breach.

j. The Intelligence Directorate for ANG, ARO-I, or NGB JS will:

(1) Provide information on potential adversary actions, indicators, and warnings, and,

(2) Provide information on Counter-Intelligence actions and requirements.

k. The Communications Directorate for ANG, ARNG, or NGB JS will monitor incidents reported to the CND Team and Help Desk to ensure any incidents involving PII have been reported to NGB-JA-OIP.

l. Directorate or Division Chief where the incident occurred will:

(1) Provide staffing to assist in response to the PII breach when an incident occurs within their area,

(2) Provide funding, if necessary, to outsource necessary services in response to a PII breach that occurs within their area to include making determination on whether to offer and pay for credit monitoring services for affected individuals,

(3) Sign and distribute written notification letters to all individuals affected by a PII breach that occurs within their area, when notification is required (see Enclosure 7), and,

(4) Attend the next quarterly PII CMG meeting and provide a roll-up summary of the incident handling.

m. The DAA will:

(1) Formally assume responsibility for continued operation of a system impacted by a PII breach. Continued operation is contingent upon reestablishing a LOW level of operational risk through mitigation of security weaknesses following a breach,

(2) Ensure the System Owner mitigates security weaknesses which contributed to the breach.

(3) Ensure that the Privacy Impact Assessment (PIA) was properly completed on the system and will be aware of the elevated operational risk levels for systems under their purview resulting from a security weakness which impacts information confidentiality.

n. The ISO will:

(1) Using a plan of Action & Milestones (POA&M) (from DoDI 8510.01, Reference N), identify and mitigate all computer asset vulnerabilities exploited in the PII breach. The ISO will coordinate POA&M mitigation strategies and timelines with the DAA or DAA representative. If circumstances warrant, they may direct that the system be monitored for misuse of the PII and for patterns of suspicious behavior,

(2) Return affected systems to an operationally ready state which may include removal of information from computer systems or Internet/Intranet pages or revising permission settings/access provisions.

ENCLOSURE 3

PII BREACH REPORTING FLOW CHART

Discoverer of PII Incident immediately reports discovery to NGB-JA-OIP (Privacy@ng.army.mil); NGB-JA-OIP will notify Directorate (where incident occurred) of reporting (when necessary).

↓

Directorate reports incident within 1 hour to US-CERT (http://www.us-cert.gov/) and completes the DoD PII Breach Report and Risk Assessment Model within 12 hours and submits to NGB-JA-OIP. Director also alerts leadership of incident.

↓

NGB-JA-OIP reviews PII Breach Report and Risk Assessment and completes overall risk assessment determination. Incident is reported to DoD, AF, or AR Privacy Office and PII IRT.

↓

NGB PII IRT will convene when determined by NGB-JA-OIP or another member of the NGB PII IRT to determine handling of incident.

↓

Directorate appoints independent investigating officer to review incident.

↓

Investigating officer reviews incident and reports findings and revised/final DoD PII Breach Report within 7 days of incident to their Director and NGB-JA-OIP to close out incident.

↓

Directorate notifies affected individuals of the PII Breach within 10 days of incident, when required, following DoD procedures.

ENCLOSURE 4

DOD PII BREACH REPORT TEMPLATE

(To Be Completed as a Word Document, Do Not Use Acronyms)

FOR OFFICIAL USE ONLY (When Completed)

MEMORANDUM FOR DEFENSE PRIVACY OFFICE

SUBJECT: Lost, Stolen, or Compromised PII Breach Report

1a. Date of Breach: DD MMM YY 1b. Breach Discovery Date: DD MMM YY

2a. US-CERT Number: 2b. Date Reported to US-CERT: DD MMM YY

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

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

4. DoD Component and organization involved:

Component Name	National Guard Bureau
Organization/ Unit Name	(Indicate Directorate name here)
POC Title/ Organization	
Commercial Phone	
Email	

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

Name	
Address	(include full unit mailing address)
Title/Organization	
Commercial Phone	
Email	

6. Total number of individuals affected by the breach: (Indicate if this is an estimate)

6a. Breakout number by category:

Government Civilians		Government Contractors	
Military (Reserve)		Military (Dependent)	
Military (Active)		Military (Retired)	
Members of Public/Other/Unknown (please specify)			

7. Did this incident involve one of the following? (Select those all 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

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)	☐	☐
Email sent to non-Federal agency	☐	☐
Other (specify)	☐	☐

7d. Type of Personally Identifiable Information involved in the incident.

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)

---------- *This section completed by NGB-JA-OIP* ----------

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.

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

Name	
Address	
Title/Organization	
Telephone	
Email	

ENCLOSURE 5

DOD RISK ASSESSMENT MODEL

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

(Each question to be answered by Directorate where incident occurred)

No.	Factor/DoD Risk Determination	Directorate's Assessment (Low, Medium, High) and Comments	Comments to consider: Low and moderate risk/harm determinations and the decision whether notification of individuals is made, rest with the Head of the DoD Component where the breach occurred. **All overall determinations (considering all 5 factors) of high risk or harm require notifications.**
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 identifier (not SSN, Medical or Financial) / **MODERATE**		Additional identifiers include date and place of birth, mother's maiden name, biometric record and any other information that can be linked or is linkable to an individual.
	c. SSN / **HIGH**		
	d. Name plus SSN / **HIGH**		
	e. Name plus Medical or Financial data / **HIGH**		
2.	Number of Individuals Affected		The number of individuals involved is a determining factor in how notifications are made, not whether they are made.
3.	What is the likelihood the information is accessible and usable?		What level of protection applied to information?
	a. Encryption (FIPS 140-2) / **LOW**		
	b. Password / **MODERATE OR HIGH**		Moderate/High determined in relationship to category of data in No. 1.
	c. None / **HIGH**		
4.	Likelihood the Breach May Lead to Harm / **HIGH, MODERATE, OR LOW**		Determining likelihood depends on the manner of the breach and the type(s) of data involved.
5.	Ability to Mitigate the Risk of Harm		
	a. Loss of information / **HIGH**		Evidence exists that PII has been lost; no longer under DoD control.
	b. Theft of information/ **HIGH**		Evidence shows that PII has been stolen and could possibly be used to commit ID theft?
	c. Compromise		
	(1) Compromise w/i DoD control / **LOW OR HIGH**		Low: No evidence of malicious intent. High: Evidence or possibility of malicious intent.
	(2) Compromise beyond DoD control / **HIGH**		Possibility that PII could be used with malicious intent or to commit ID theft.

ENCLOSURE 6

RISK OF HARM CONSIDERATIONS

1. Introduction.

a. The policies established by OMB and DoD (Encl 8 References C, L, and O) require that a determination be made on all PII breaches as to whether the breach of PII puts an affected individual at risk of harm. If there is a high risk of harm and a high level of impact, the OMB and DoD policies require that affected individuals be notified of the incident. If there is a medium risk of harm or level of impact, the notification to affected individuals is at the discretion of the agency. The DoD Risk Assessment Model (Encl 5) will be used as a tool to analyze the risk of harm and level of impact and assist in determining whether or not to notify the affected individuals.

b. The directorate where the incident occurred will assign a low, moderate, or high risk of harm determination to each factor using the DoD Risk Assessment Model. The NGB-JA-OIP will make the overall risk determination and report the determination on the DoD PII Incident Report (Encl 4). This determination will determine when and how NGB should notify affected individuals.

2. Factors to Consider in Determining Risk.

a. NGB considers the specific facts, circumstances, context of the breach, National Institute of Standards & Technology (NIST) standards (Encl 8, Reference F; note: this does not apply to National Security Systems), and DoD Guidance (Encl 8, References L and O) to evaluate the likely risk of harm and the level of impact. NGB uses this information to determine whether it should provide notice to affected individuals and to determine the nature and extent of notice.

b. The fact that information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. If information is properly protected (e.g., consistent with NIST standards) the risk of compromise may be low to non-existent.

3. Factors to Determine the Risk of Harm.

a. 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 the names of individuals in conjunction with whole or partial 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. In

assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

b. Number of Individuals Affected. The magnitude of the number of affected individuals may dictate the method you choose for providing notification, but is not a determining factor for whether or not notification will be made.

c. Likelihood the Information is Accessible and Usable.

(1) Upon learning of a breach, an assessment on the likelihood the PII can be or has been used by unauthorized individuals must be made. An increased risk that the information can be used by unauthorized individuals will influence the NGB's decision on providing notification.

(2) 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 the NIST. The NGB will assess whether the breach involving personally identifiable information is at a low, moderate, or high risk of being used by unauthorized persons to cause harm to an individual or group of individuals using the DoD Risk Assessment Model and will consider the likelihood any unauthorized individual will know the value of the information and either use or sell the information to others.

d. Likelihood the Breach May Lead to Harm.

(1) Broad Reach of Potential Harm. 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, NGB 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 information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

(2) 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 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 personally identifying information, 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, NGB will consult guidance issued from the Identity Theft Task Force found at http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

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

ENCLOSURE 7

BREACH NOTIFICATION CONSIDERATIONS

1. Notification.

a. In situations when there is little or no risk of harm, NGB generally will not issue notice. When the risk of harm is low, NGB also will consider the costs to individual and businesses, e.g., financial institutions, associated with responding to notices.

b. In deciding whether to provide notice, NGB should give greater weight to the likelihood that the PII is accessible and usable and to the likelihood that the breach may lead to harm. In analyzing the factors (Encl 6) in a fact specific context, it is likely that NGB only will provide notification in instances where there is a likely a high risk of harm.

2. When and who to notify.

a. NGB gives notice to affected individuals without unreasonable delay but no later than 10 days of determining who will be notified and obtaining the contact information for individuals being notified. Permissible delays are limited only to those situations that involve law enforcement or national security considerations, or the need to restore the integrity of information systems prior to notification. Decisions to delay notification will be made by the CNGB or his/her designee and a notice of the delay will be given to the Defense Privacy Office.

b. The NGB PII IRT will determine if NGB needs to notify any third parties; e.g., those with oversight responsibilities, other agencies that may be affected by the breach and/or agencies that may help mitigate the breach, members of the public, and/or the media. Notifications must be compliant with Section 508 of the Rehabilitation Act which requires Federal agencies to make their electronic and information technology accessible to people with disabilities. This may require NGB to establish a Telecommunications Device for the Deaf (TDD) and/or to post a large print notice on the NGB web site.

3. Content of Notification.

a. NGB will use plain language in all notifications and will include the following information in all breach notification materials, regardless of the medium or method:

1) An apology;

2) A brief description of what happened, including the date(s) of the breach and the date that NGB discovered it;

3) A description of the types of PII involved in the breach (e.g., full name, social security number, date of birth, home address, disability information);

4) A statement on whether the information was protected using NIST and/or DoD standards;

5) What steps individuals might wish to take to protect themselves from potential harm;

6) What NGB is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and

7) Who affected individuals should contact for more information, which may include a toll-free telephone number, and/or postal address.

b. A sample letter for completing notifications to affected individuals can be found in DoD 5400.11-R (Encl 8, Reference L).

4. NGB Official Responsible for Notification. The Director, where the incident occurred, or a higher authority, will sign the written notices that are sent to individuals.

5. How to notify. Consistent with DoD 5400.11-R, the best means for providing notification will depend on the number of individuals affected and what contact information is available about the affected individuals. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. NGB will consult with the General Services Administration's (GSA) USA Services for outsourcing when necessary (1-800-333-4636, www.USA.gov). The following examples are types of notices that NGB may use exclusively or in combination:

a. Telephone. Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. In accordance with DoD's Director of Administration and Management (DA&M) Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", June 5, 2009 (Encl 8, Reference O), in such instances that individuals are notified by phone, the notification must be followed-up by a written notification.

b. First-Class Mail. This is the preferred means of notification for NGB. NGB will send the notice separately from other National Guard mailings so that it is obvious to the recipient that it pertains to the National Guard and that the matter is urgent. The mailing will comply with OMB and DoD Policy to include markings on the front of the envelope to alert the recipient to the importance of its contents.

c. Electronic –Mail. The NGB may use E-mail notification exclusively only if the individual has provided an e-mail address to us and expressly has given his consent to use e-mail as the primary means of communication with the National Guard. The NGB may use e-mail in conjunction with written notice if the circumstances of the breach warrant such an approach. E-mail notification may also include links to the NGB

website to obtain more information on the incident or assistance and may also contain links to approved web sites (found at www.USA.gov). Notices to individuals will be "layered" so that the most important summary facts are up front with additional information provided under link headings.

d. Web Posting. Depending on the circumstances, NGB may post information about the breach and notification on our home page at http://www.ng.mil. The posting may include a link to Frequently Asked Questions (FAQs) and other information to assist the public's understanding of the breach and of the notification process. The website may also include links approved and posted by the www.USA.gov web site.

e. Newspapers or other Public Media Outlets. In rare circumstances, NGB may supplement individual notice with notifications in newspapers or other public media outlets. NGB may use toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.

f. Substitute Notice. The NGB may use substitute notice in those instances where it does not have sufficient contact information to provide another means of notification. Substitute notice may consist of a conspicuous posting of the notice on the home page of the NGB web site at http://www.ng.mil/ and/or notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media may include a toll-free phone number where an individual can find out more information about the incident.

6. Breaches involving contractors. If the breach involves a Federal contractor or a public-private partnership operating a system of records on our behalf, NGB will determine who is responsible for costs and labor of notification and ensure that other corrective actions are taken as appropriate. The NGB includes appropriate Federal Acquisition Regulation language regarding Federal Information Security Management Act requirements and PII loss reporting responsibilities in all contracts and other acquisition documents.

ENCLOSURE 8

REFERENCES

A. Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. § 3541)

B. The Privacy Act of 1974, as amended (5 USC § 552a)

C. Office of Management and Budget (OMB) Memorandum M-07-16, "Safeguarding Against & Responding to the Breach of Personally Identifiable Information," 22 May 07

D. Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems", Feb 04

E. FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems", Mar 06

F. National Institute of Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems"

G. NIST Special Publication 800-61, "Computer Security Incident Handling Guide", 26 Jan 06

H. Chairman of the Joint Chiefs of Staff Manual 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," Change 3, 8 Mar 06

I. DoD Directive O-8530.1, "Computer Network Defense (CND)", 8 Jan 01

J. DoD Directive 5105.77, "National Guard Bureau," 21 May 08

K. DoD Directive 5400.11, "DoD Privacy Program," 8 May 07

L. DoD Regulation, 5400.11-R, "DoD Privacy Program," 14 May 07

M. DoD Instruction 8500.2, Information Assurance Implementation, 6 Feb 03

N. DoD Instruction, 8510.01, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction, 28 Nov 07

O. DoD Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)," 5 Jun 09 (www.defense.gov/privacy)

ENCLOSURE 9

DEFINITIONS

A. Breach. From the Office of Management and Budget memorandum M-07-16 (Reference C): A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where a person other than authorized users (with an official need to know), and for an other than authorized purpose has access or potential access to personally identifiable information, whether physical or electronic. A breach can include identifiable information in any form.

B. Harm. Specifically: physical, psychological, or economic injury or damage that could come as a result of a breach. Breaches can implicate a broad range of harms to individuals, including the potential for economic or medical identity theft. OMB requires agencies to consider a wide range of harms associated with the loss or compromise of information, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach. Such harms may also include the effect of a breach of confidentiality on 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.

C. Identity Theft. Identity theft and identity fraud are terms used to refer to all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

D. Level of Impact. Impact levels - low, moderate, and high - describe the worst case potential impact on an organization or an individual, if a breach of security occurs. The DoD Senior Agency Official for Privacy has provided risk level guidance in the 5 Jun 09 Memorandum (Reference O) and impact levels have been defined by the NIST are as follows:

- Low: The loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

- Moderate: The loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

- High: The loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

E. Lost, stolen, or compromised PII. From DoD 5400.11-R (Reference L): 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 other than authorized purposes where one or more individuals will be adversely affected.

F. Personally Identifiable Information (PII). From DoD Directive 5400.11 (para E2.e) (Reference K) and DoD 5400.11-R (para DL1.14) (Reference L): Information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., a social security number (full or partial); age; military rank; civilian grade; marital status; race; salary; home/office/cell phone numbers and other demographic, biometric, personnel, medical, and financial information). Such information can be used to distinguish or trace an individual's identity and includes other personal information which is linked or linkable to a specified individual.

G. PII Incident Response Team (IRT). An advisory team comprised of stakeholders and experts trained in responding to incidents involving the loss, theft, or compromise of PII.

H. Risk. With regard to a breach of PII, risk is defined as the likelihood of injury or harm caused to an individual whose PII is the subject of such breach.