OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

ADMINISTRATION AND
MANAGEMENT

AUG 2 2012

MEMORANDUM FOR COMPONENT PRIVACY OFFICERS

SUBJECT: Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations

References: (a) Director, Administration and Management Memorandum "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," June 5, 2009
(b) Office of Management and Budget Memorandum, M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investment," July 21, 2006
(c) DoD 5400.11-R "Department of Defense Privacy Program," May 14, 2007
(d) DoDD 5400.11 "DoD Privacy Program," May 8, 2007
(e) National Institute of Standards and Technology (NIST) Special Publication 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information," April 2010

The purpose of this memorandum is to help guide Components toward optimal decision-making regarding PII breach risk and notification determinations as described in references (a), (c), and (d). It also replaces Table 1 of reference (a).

The Department must continue its efforts to promote a culture to continuously 'think privacy' and act swiftly to develop and implement effective breach mitigation plans, when necessary. Our challenge is that no two breaches of PII involve the exact same circumstances, personnel, systems, or information. A case-by-case analysis combined with the use of best judgment is required for effective breach management.

The determination whether to notify individuals of a breach is based on an assessment of the likelihood that the individual will be harmed as a result of the breach and its impact. Harm includes embarrassment, inconvenience, financial loss, blackmail, identity theft, emotional distress and loss of self-esteem. Five factors should be weighed to assess the likely risk of harm:

- Nature of the data elements breached
- Number of individuals affected
- Likelihood the information is accessible and usable
- Likelihood the breach may lead to harm, and
- Ability of the Department to mitigate the risk of harm.

A final decision regarding whether to make notification cannot be made until after each factor has been assessed. The decision to notify should not be based on one factor alone. For example, a breach may involve social security numbers (SSNs) making that factor a high risk.

However, SSNs may be stored on an encrypted, Common Access Card-enabled laptop to mitigate potential compromise which could lead to harm. Therefore, although one factor in this example (data elements) rates as a high likelihood of harm, after all factors are evaluated and considered, the overall likelihood of harm resulting from the breach is low given the technical safeguards in place. Generally, absent other factors, Components should not notify personnel of breaches that have a low overall likelihood of harm.

Components should remain cognizant of the effect that unnecessary notification may have on the public. Notification when there is little or no risk of harm might create unnecessary concern and confusion. Additionally, overzealous notifications resulting from notification criteria which are too strict could render all such notifications less effective because consumers could become numb to them and fail to act when risks are truly significant.

Questions regarding this memorandum should be directed to Samuel P. Jenkins, Director for Privacy, Defense Privacy and Civil Liberties Office at (703) 571-0070 or sam.jenkins@osd.mil.

Michael L. Rhodes
DoD Senior Official for Privacy