DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

NOV 30 2018

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Reporting of Breaches of Personally Identifiable Information in Accordance with the Department of Defense Breach Response Plan

The purpose of this memorandum is to remind DoD personnel of their obligation to respond to known or suspected breaches of personally identifiable information (PII) in accordance with the attached DoD Breach Response Plan.

A breach of PII is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.

DoD is committed to protecting an individual's privacy when maintaining his or her PII. As a Department, we must remain cognizant of the effect that failures to respond to breaches of PII may have on Department activities and the public, including impairment of mission critical functions, compromise of sensitive data, and harm to impacted individuals.

I encourage each of you to familiarize yourself with the current DoD Breach Response Plan. Questions regarding the plan should be directed to Cindy Allard, Chief, Defense Privacy, Civil Liberties, and Transparency Division, at (703) 571-0070.

Patrick M. Shanahan

Attachment:
As stated

OSD015767-18/CMD020047-18

Effective September 28, 2017

THE DEPARTMENT OF DEFENSE

BREACH RESPONSE PLAN

PURPOSE. The Department of Defense (DoD) reporting process is to be used when there is a known or suspected loss of DoD personally identifiable information (PII). It includes new and existing requirements issued by the Office of Management and Budget (OMB) Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017). This DoD breach response plan shall guide Department actions in the event of a breach of personally identifiable information (PII).

SCOPE. Applies to all DoD personnel to include all military, civilian and DoD contractors.

Does **not** apply to national security systems as defined in 44 U.S.C. §3552 (b)(6). However, DoD Components operating national security systems are encouraged to apply this plan to those systems if practicable.

1. DOD BREACH RESPONSE TEAM

a. General. The Secretary of Defense or designee will designate a DoD Breach Response Team ("Team") at the department level, to review, assess, and respond to breach of PII. The Team will meet annually, for a Tabletop exercise, and when a breach constitutes a major incident. In that regard, it will adhere to the following guidelines:

A breach constitutes a major incident when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a major incident as defined in OMB Memorandum M-17-05, *Fiscal Year 2016 – 2017 Guidance on Federal Information Security and Privacy Management Requirements*, page 8. *Note*: *Unauthorized exfiltration* is defined as the act or process of obtaining, without authorization or in excess of authorized access, information from an information system without modifying or deleting it.

b. Membership. The Team will include the Senior Agency Official for Privacy (SAOP), the Chief Information Security Officer (CISO), the Chief, Defense Privacy, Civil Liberties, and Transparency Division, (DPCLTD) and representatives of the following offices: The DoD Office of General Counsel (OGC), the Office of the Assistant Secretary of Defense, Legislative Affairs (OASD(LA)), and the Office of the Assistant to the Secretary of Defense for Public Affairs (OASD(PA)). Other personnel, to include senior intelligence officers, national security advisors and law enforcement personnel, may be added to the Team as appropriate.

2. TEAM MEMBER RESPONSIBILITIES

a. The SAOP, as Team lead, will:

(1) Convene the Team when appropriate, and at least once per year;

(2) Coordinate with the Senior Component Official for Privacy (SCOP) and DoD OGC over their determination on whether a major incident has occurred;

(3) Determine and coordinate with financial management personnel the resources to be allocated as a result of a major breach incident, and advise the DCMO accordingly.

(4) Report the major breach to the appropriate Congressional Committees[1] within seven (7) days after the date on which there is a reasonable basis to conclude that a breach has occurred. At the time of submission, such a report (and any supplemental report) must include:

(a) A summary of information available about the breach, including how the breach occurred;

(b) The sensitivity or the security classification of the information breached;

(c) An estimate of the number of individuals affected by the breach, including an assessment of the risk of harm to affected individuals;

(d) A description of any circumstances necessitating a delay in providing notice to affected individuals; and

(e) An estimate of whether and when the agency will provide notice to affected individuals.

(5) In addition, the SAOP will ensure supplementary information is provided to the requisite Congressional Committees within a reasonable time after the information is uncovered, but not later than 30 days after the initial report of the major breach. The supplement must include:

(a) Threats and threat actors, vulnerabilities, and impacts related to the incident;

(b) The risk assessments conducted of the affected information systems prior to the incident;

(c) The status of compliance of the respective information system(s) with security requirements in place at the time of the major incident; and

(d) The detection, response, and remediation actions.

[1] OMB Memorandum 17-05, "Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements," pages 9.

b. The CISO will:

(1) Serve as the principal Information Technology/Cybersecurity point of contact (POC) for major breach incidents;

(2) Evaluate the effectiveness of information security measures in place to protect the potentially breached PII;

(3) Provide a determination of the likelihood and extent of the major breach, to include the data sets compromised and the number of individuals affected;

(4) Evaluate the effectiveness of information security mitigating actions.

c. The DoD Office of General Counsel (OGC) will:

(1) Provide legal advice to the Team;

(2) Provide an opinion on the appropriateness of individual notification;

(3) Provide input on whether the major breach must be reported to the Congressional Committees designated by OMB;

(4) Provide input on the appropriateness of notification to the media.

d. The Office of the Assistant Secretary of Defense, Legislative Affairs will:

(1) Provide guidance when the major breach must also be reported to the Congressional Committees;[2]

(2) Review and oversee the transmission of DoD's initial and supplemental major breach incident reports to Congress.

e. The Office of the Assistant to the Secretary of Defense, Public Affairs will:

Provide specific guidance on how to effectively communicate the details of a major breach incident to the public and the media, when appropriate.

f. The Chief, DPCLTD, upon notification of any breach will:

(1) Serve as a liaison between the affected component, the SAOP, and the Team;

(2) Provide the SAOP with information regarding the numbers and types of major breaches throughout DoD;

---

[2] OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," page 20.

(3) Provide an analysis of trends in major breach incidents and possible preventive measures;

(4) Assist the SCOP and Component Privacy Officer (CPO) and monitor the actions of the component in response to the breach.

Reporting Exceptions. If reporting the suspected or confirmed breach will seriously impede a criminal investigation or national security interests, then a law enforcement, cybersecurity, or national security organization may request a postponement of the reporting requirement until such time as the SAOP can evaluate and mitigate the impact on essential DoD missions.

3. COMPONENT OFFICIAL BREACH RESPONSIBILITIES

a. General. Consistent with OMB Guidelines, the SCOP will be responsible for the management of breaches at the component level with support from the CPO. The SCOP will inform the Chief, DPCLTD of breaches to ensure a seamless flow of information throughout the department when any breach occurs. If it is determined that the breach was not a major incident, the SCOP is the lead and will share required information within the agency and determine the actions to be taken, ensuring, that DPCLTD is updated as information becomes available. If it has been determined to be a major breach incident the Chief, DPCLTD will inform the SAOP.

b. The SCOP will:

(1) Determine along with OGC, and in consultation with the CPO, if a major incident breach has occurred;

(2) Conduct and document an assessment of the risk of harm to individuals potentially affected by a breach;

(3) Determine how to best mitigate the harm to individuals affected by a breach;

(4) Determine whether to notify individuals potentially affected by the breach; in notifying individuals the SCOP will consider the Source, Timeliness, Content, Method, and any Special Considerations necessary regarding the notification.

(5) Determine appropriate actions in response to a breach, to include countermeasures, additional staff resources when appropriate, and guidance or services to individuals potentially affected; and

(6) Ensure that law enforcement and Offices of the Inspectors General and component General Counsel receive timely notification when notification is appropriate.

c. CPO Actions. The CPO, or designated staff member, in addition to sharing information with the SCOP regarding the breach, will ensure that all required reporting occurs. The CPO, or designated staff member, will report the details on the suspected and actual breach incidents to the respective SCOP within 24 hours of breach discovery and report suspected or confirmed computer breach incidents to US-CERT within 1 hour if the breach involves a confirmed

cybersecurity incident at https://www.us-cert.gov/forms/report. In addition, the CPO, or designated staff member, will:

(1) Provide the SCOP with the system of records notices (SORNs), Privacy Impact Assessments, and privacy notices applicable to the potentially compromised information;

(2) Document all breaches and actions taken in response to a breach using the DD Form 2959, and submit it to DPCLTD via the Compliance and Reporting Tool (CART);

(3) Notify DPCLTD within 48 hours of discovery of a breach incident;

(4) Update initial reports in CART as information becomes available and/or as pertinent decisions are made. This includes documenting whether affected individuals are being notified and, if so, the form of notification and the number of affected individuals notified; and

(5) Close breach reports in CART when all actions are complete.

4. MODEL ROUTINE USES. To facilitate responses to breach incidents the following routine uses will be added to all DoD component SORNs:

a. "To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm."

b. "To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach."

5. PLAN AND REFERENCES.

a. General. This Breach Response Plan will be reviewed on an annual basis by the SAOP and the Chief, DPCLTD.

b. Reference Documents. The following documents provide additional background, definitions, and understanding of this plan:

(1) OMB Memorandum M-17-05, "Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Documents," November 4, 2016;

(2) OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017;

(3) OMB Memorandum M-16-14, "Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response," July 1, 2016.