THE UNDER SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

February 12, 2019

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Department of the Navy Breach Response Plan

Reference: DON CIO Washington DC 291652Z Feb 08, Loss of Personally Identifiable Information Reporting Process

The purpose of this memorandum is to establish Department of the Navy (DON) policy in the event of a known or suspected loss of DON personally identifiable information. It applies to all DON personnel in the Secretariat, Navy, and Marine Corps including military members, civilian personnel, and DON contractors. The attached breach response plan supersedes the reference.

The DON point of contact is Mr. Steve Muck, who can be reached at (703) 695-1297 or via email at steven.muck@navy.mil.

Thomas B. Modly

Attachment:
As stated

Distribution:
ASN (RD&A)
OGC
CNO
CMC
DUSN
DASN (CHR)
DNS
DMCS
AUDGEN
OCIO
NCIS
NAVIG
IGMC
OJAG
OLA
CHINFO

THE DEPARTMENT OF THE NAVY

BREACH RESPONSE PLAN FOR THE LOSS OF PII

PURPOSE. The Department of the Navy (DON) breach response plan (BRP) is to be used when there is a known or suspected loss of DON personally identifiable information (PII). It includes new and existing requirements issued in 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). The DON BRP aligns with the Department of Defense (DoD) BRP, dated September 28, 2017 and will guide DON actions in the event of a breach of PII. This plan supersedes DON CIO WASHINGTON DC 291652Z FEB 08, LOSS OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORTING PROCESS.

SCOPE. This plan applies to all DON personnel, including military, civilian, and DON contractors.

1. DON BREACH RESPONSE TEAM (BRT)

a. General. The DON Senior Component Official for Privacy (SCOP) will designate and lead the DON BRT at the department level, when a breach constitutes a major incident. The BRT will conduct DON tabletop exercises (TTXs) at least annually. The purpose of the TTX is to test the DON PII breach response process, identify breach policy and process gaps, and to refine and validate the plan.

b. Membership. The BRT will include the:

- DON SCOP
- DON Office of the Chief Information Officer (OCIO) Privacy Team
- Deputy Under Secretary of the Navy (DUSN) Senior Director for Security (SDS)
- Deputy Assistant Secretary of the Navy for Civilian Human Resources (DASN (CHR))
- DON Office of General Counsel (OGC)
- Navy Office of Information (CHINFO)
- DON Office of the Judge Advocate General (OJAG)
- DON Office of Legislative Affairs (OLA)
- DON Assistant for Administration (DON AA)
- DON AA Counsel

In addition, and as appropriate for:

- Navy Breaches
  - Chief of Naval Operations (OPNAV N2N6)
  - Director Navy Staff (DNS-36)
  - Naval Inspector General (NAVINSGEN)
  - Naval Audit Service (NAVAUDSVC)
  - U.S. Fleet Cyber Command (USFLTCYBERCOM)

- the accountable command (i.e., command or activity responsible for causing the breached PII)

- Marine Corps Breaches
  - Headquarters Marine Corps (HQMC C4)
  - Director of the Marine Corps Staff (DMCS ARSF)
  - Office of U.S. Marine Corps Communications (OMCC)
  - Inspector General of the Marine Corps (IGMC)
  - Marine Corps Audit Service (MCAUDSVC)
  - U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER)
  - the accountable command

- Other Navy or Marine Corps organizations may be added to the BRT, as appropriate.

2. ACTIONS BASED ON NUMBER OF IMPACTED INDIVIDUALS

Upon receipt of an initial breach report (i.e., SECNAV Form 5211/1, Loss or Compromise of Personally Identifiable Information (PII)) the DON OCIO Privacy Team will review the report and determine which of the following will occur:

a. 100,000 or More Individuals Impacted (i.e., Major Incident)

The DON SCOP, DON OGC, and DON OCIO Privacy Team, upon confirmation that a suspected or confirmed PII breach impacts potentially 100,000 or more individuals or is likely to result in demonstrable harm to 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, will notify the DoD Senior Agency Official for Privacy (SAOP) through the Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). The SAOP will convene the DoD BRT and coordinate the breach response, risk analysis, individual notification determination, and Congressional notification with the DON SCOP and DON OCIO Privacy Team.

b. 10,000 up to 99,999 Individuals Impacted

The DON OCIO Privacy Team, upon confirmation that a suspected or confirmed PII breach potentially impacts from 10,000 up to 99,999 individuals, will notify the DON SCOP. The DON SCOP and DON OCIO Privacy Team will determine whether the circumstances of the breach warrant convening the DON BRT. The BRT, if convened, will coordinate the breach response. Based on their risk analysis, the BRT will determine whether individual notifications are required. The DON OCIO Privacy Team will notify the DPCLTD of the breach.

c. Less than 10,000 Individuals Impacted

The DON OCIO Privacy Team, upon confirmation that a suspected or confirmed PII breach potentially impacts less than 10,000 individuals, will work with the reporting command, perform a risk analysis, and make an individual notification determination.

The DON OCIO Privacy Team may notify the DPCLTD of the breach depending on the specific circumstances of the breach.

3. TEAM MEMBER RESPONSIBILITIES

a. The SCOP will:

(1) Convene the DON BRT when appropriate, and at least once per year to conduct a TTX;

(2) Recommend to the SAOP on whether a major incident has occurred;

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

(4) Delegate individual notification responsibilities to the respective service.

(5) When necessary, resolve disputes between commands and assign breach reporting and individual notification responsibilities.

(6) Coordinate with the SAOP to report the major breach to the appropriate congressional committees within seven (7) days after the date on which there is a reasonable basis to conclude that a major 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 DON will provide notice to affected individuals.

(7) In addition, ensure supplementary information is provided to the SAOP for reporting 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.

(8) Ensure that law enforcement, the Naval Inspector General or Inspector General of the Marine Corps and DON General Counsel receive timely notification when appropriate.

(9) Direct forensics support services be obtained when a breach involves the suspected or actual infiltration of an IT system for malicious purposes.

(10) Direct that identity protection services (IPSs) be provided in accordance with paragraph 5.

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

b. U.S. Fleet Cyber Command (USFLTCYBERCOM) or HQMC DCI/C4 Cybersecurity Division 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 DON Office of General Counsel (OGC) will:

(1) Provide legal advice to the SCOP and BRT;

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

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

d. The DON Office of Legislative Affairs (OLA) will:

Coordinate with the DPCLTD when a breach requires notification to the congressional committees designated by OMB.

e. The Navy Office of Information (CHINFO) and/or the Office of U.S. Marine Corps Communications (OMCC) 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. Space and Naval Warfare Systems Command (SPAWAR) Systems Center Atlantic Cyber Forensics Investigations (CFIX) Laboratory will:

Provide forensics support when requested in support of PII breaches involving the compromise of information due to malicious activity.

g. The DON OCIO Privacy Team, upon notification of any breach will:

(1) Serve as a liaison between the affected DON organization/command and the SCOP;

(2) Provide the SCOP with information regarding the numbers and types of breaches throughout the DON;

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

(4) Monitor the actions of the affected DON organization/command in response to the breach.

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

(6) Receive breach reports from DON commands and organizations. Make and document a notification determination by assessing the risk of harm to individuals potentially affected by the breach. When warranted, recommend the SCOP convene the BRT in order to respond to the breach and mitigate its impact to potentially affected individuals;

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

(8) Based on a risk analysis, direct individual notifications.

h. Secretariat, Navy, and Marine Corps Accountable Commands will:

(1) Follow the breach reporting process in the table of paragraph 4.

(2) Take necessary actions to mitigate the breach and prevent reoccurrence.

(3) Investigate the cause of the breach.

(4) Ensure individual notifications are made when directed.

(5) Provide IPS when directed.

(6) Identify lessons learned.

Reporting and Notification Exceptions. If reporting a suspected or confirmed breach, or if individual notifications will seriously impede a criminal investigation or national security interests, then a law enforcement, cybersecurity, or national security organization may request a delay in making individual notifications until such time as the SCOP can evaluate and mitigate the impact on essential DON missions.

4. BREACH REPORTING PROCESS

The following table summarizes the DON PII breach reporting process and required actions:

Responsible Organization	Time Frame	Action	References and Resources
Discovering Command	—	PII breach is confirmed or suspected	OMB Memorandum M-17-12
Discovering Command	Within one hour	Report breach to DON OCIO Privacy Team, NCCIC (U.S. CERT), DNS, HQMC C4, chain of command as appropriate, and law enforcement (if criminal intent is indicated)	• SECNAV 5211/1 Breach Report
DON OCIO Privacy Team	Within 24 hours	• Assign tracking number • Conduct risk analysis • Make individual notification determination • Initiate Breach Response Team (if appropriate) • Determine if a major incident • Send report to CHINFO, OGC, OJAG, NCIS, FLT CYBER, DUSN (P) Security, N1, as applicable • Recommend procurement of IPSs (if applicable).	DON Risk Analysis Methodology in accordance with OMB M-17-12
DON OCIO Privacy Team	Within 48 hours	Notify DPCLTD of breach.	
Accountable Command	Within 10 days	Send notification letter to each affected individual (if directed)	Sample breach notification letter on the DON CIO website PII Breach Reporting Resources page
Accountable Command	If required	Provide identity theft protection services (if applicable)	GSA Blanket Purchase Agreements for federal agencies.
Accountable Command	Within 30 days	Close out breach with After Action Report to DON OCIO Privacy Team	SECNAV 5211/2 After Action Report

When applicable, issue an OPREP-3 in accordance with OPREP-3 reporting procedures.

Exceptions. The following do not require a PII breach report to be submitted due to the associated low risk of harm:

- The loss or compromise of an individual's DoD ID Number, by itself, when associated with the individual's name, or as part of their digital signature.
- The loss or compromise of an individual's own PII.
- The release, loss, or compromise of PII that is normally releasable without a clearly unwarranted invasion of personal privacy, including an individual's office information (e.g., full name, office email address, office phone number, office address, pay grade/rank, DoD ID number).

- An unencrypted email containing PII, in the body of the email or as an attachment, remains within the .mil network and all recipients have an official need to know.

- In the case of the loss or theft of removable storage media, including laptops, mobile devices, and tablets, that are confirmed by the organization's Information Systems Security Manager (ISSM) to be enabled with DoD approved data-at-rest (DAR) software.

5. IDENTITY PROTECTION SERVICES (IPS).

a. When responding to a PII breach, the DON OCIO Privacy Team will make the determination for IPS upon consideration of the following requirements:

(1) The PII breach was reported to the DON Privacy Office in accordance with current policy;

(2) The PII data was maintained by a DON Command or under a DON contract;

(3) The DON Privacy Office determined the breach created a high risk of harm which required notification to the affected individual(s);

(4) The loss or compromise of PII was due to a malicious act (e.g., theft, computer hacking, insider threat).

b. For PII breaches classified as a "major incident" the Navy or Marine Corps may offer IPS to affected individuals even if not directed by the DON SCOP or the DoD SAOP.

c. For PII breaches affecting 10,000 up to 99,999 individuals, the DON BRT will determine if IPS is offered to affected individuals.

d. The following additional requirements apply when IPS is directed:

(1) IPS is authorized for a minimum of one year;

(2) IPS must be offered as an "opt-in" service (express permission by the affected individual):

(3) Affected individuals who already subscribe to a U.S. Government provided IPS should be advised that having two services in effect may not be advantageous;

(4) Only Blanket Purchase Agreements (BPA) listed on the General Services Administration (GSA) schedule may be used to purchase IPS;

(5) The accountable command will bear the cost of providing IPS to the affected individual(s) and;

(6) In breaches where a contractor is responsible for the breach of PII data managed under a DON contract, the vendor may be held responsible for the cost of IPS in accordance with the terms and conditions of the contract.

6. PLAN AND REFERENCES.

a. General. This Breach Response Plan will be reviewed on an annual basis by the SCOP and the DON OCIO Privacy Team.

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

(1) OMB Memorandum M-18-02, "Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements," October 16, 2017;

(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.

7. DEFINITIONS.

a. Accountable Command. The DON command or organization that caused the breach. The accountable command is responsible for all follow on reporting and breach mitigation actions.

b. Discovering Command. The DON command or organization that first identifies that a suspected or actual breach of PII has occurred. The discovering command is responsible for submitting the initial breach report within one hour of breach discovery.

c. Major Incident. 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.

d. Risk of Harm. The likelihood that a breach of an individual's PII will result in negative consequences to the individual (i.e., embarrassment, physical harm, financial loss, identity theft/fraud, etc.).