



Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-611
Phone: (202) 475-3519
Fax: (202) 475-3929

COMDTINST 5260.5
9 OCT 2007

COMMANDANT INSTRUCTION 5260.5

Subj: PRIVACY INCIDENT RESPONSE, NOTIFICATION, AND REPORTING PROCEDURES FOR PERSONALLY IDENTIFIABLE INFORMATION (PII)

- Ref:
- (a) Privacy Act of 1974, 5 U.S.C. § 552a
 - (b) The Federal Information Security Management Act (FISMA) of 2002, Title III of the E-Government Act of 2002, Pub. L. No. 107-347
 - (c) OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
 - (d) DHS Privacy Incident Handling Guidance (PIHG), September 10, 2007

1. PURPOSE. This Instruction provides the Coast Guard’s policy for privacy incidents.
2. ACTION. Area, district, and sector commanders, commanders of maintenance and logistics commands, commanding officers of integrated support commands, commanding officers of headquarters units, assistant commandants for directorates, Judge Advocate General, and special staff elements at Headquarters shall ensure compliance with the provisions of this Instruction. Internet release is authorized.
3. DIRECTIVES AFFECTED. None.
4. DISCUSSION. There have been a number of recent incidents where PII maintained by Federal agencies has been lost, stolen, or compromised. Disclosure of PII can result in a broad range of harm to individuals, including identity theft. This elevated risk has prompted the promulgation of procedures for responding to privacy incidents. Individuals who utilize or have contact with PII are responsible for protecting it from disclosure, loss, or misuse.
5. DEFINITIONS.
 - a. Breach. Loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where users have access or potential access to information for other than an authorized purpose.

DISTRIBUTION – SDL No. 147

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	2	2	2	1	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1					
B	1	8	20	1	12	3	10	10	3	10	3	3	2	10	1	2	2	25	1	2	2	1	3	1	1	1
C	3	2	1	3	1	1	1	1	1	1	3	1	2	2	25	1	1	1	3	1	1	1	2	1	1	1
D	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
E	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
F																	1	1	1							
G	1	1	1	1	1																					
H	1																									

NON-STANDARD DISTRIBUTION:

- b. Identity Theft. Unauthorized use of an individual's PII in an attempt to commit fraud or other crimes.
 - c. Personally Identifiable Information (PII). Data that can be used to distinguish or trace a person's identity, or any other personal information that can be linked to a specific individual. Examples of PII include: name, date of birth, home mailing address, telephone number, social security number, home e-mail address, zip code, account numbers, certificate/license numbers, vehicle identifiers (including license plates), uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, any unique identifying number or characteristic, and other information where it is reasonably foreseeable that the information will be linked with other personal identifiers of the individual.
 - d. Privacy Incident. Loss of control, breach, compromise, unauthorized disclosure/acquisition/access, or any similar term referring to situations in which unauthorized users have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both suspected and confirmed incidents involving PII.
 - e. Coast Guard Computer Incident Response Team (CGCIRT). The Coast Guard entity that must be notified upon discovery of a privacy incident. Commanding Officers must report all privacy incidents—both potential and confirmed—to the CGCIRT.
 - f. Department of Homeland Security-Security Operations Center (DHS-SOC). An entity within DHS to which the CGCIRT reports incidents. The DHS-SOC reports to the U.S. Computer Emergency Readiness Team (US-CERT).
 - g. US-CERT. The Federal Incident Response Center within DHS.
6. BACKGROUND. The continuing advancement of Information Technology has vastly increased the volume of PII maintained and the types of media upon which it is utilized, stored, and transmitted. A negative consequence of this enhanced technology is that it enables more opportunities for PII to be lost, stolen, or otherwise compromised. Privacy incidents can occur at any time and place when appropriate safeguards have not been followed. These losses have prompted the Office of Management and Budget (OMB) to inform agencies of their responsibilities relative to safeguarding PII and ensuring associated training requirements for their personnel.
- a. Privacy Act. Reference (a) mandates agencies to establish administrative, technical, and physical safeguards to ensure the integrity of records maintained on individuals. It requires the protection against any anticipated threats which could result in substantial harm, embarrassment, or compromise to an individual.
 - b. Federal Information Security Management Act (FISMA). Reference (b) requires agencies to report security incidents to a Federal incident response center- the U.S. Computer Emergency Readiness Team (US-CERT)- within one hour of discovery. US-CERT is located within DHS. The CGCIRT provides centralized reporting of all Coast Guard Privacy Incidents to DHS.

7. POLICY AND RESPONSIBILITIES. Coast Guard personnel shall report ALL privacy incidents to their Commanding Officer immediately upon discovery—regardless of whether the incident has been confirmed or is merely suspected. This reporting requirement applies to all Coast Guard personnel, including active duty, reserve, civilian employees, independent consultants, and government contractors who use, or have access to, Coast Guard information resources. The Commanding Officer shall forward ALL privacy incident reports to the CGCIRT and shall not distinguish between suspected and confirmed privacy incidents.
8. PROCEDURES. These procedures ensure Coast Guard and DHS officials responsible for safeguarding PII in accordance with references (c) and (d) are fully informed of a privacy incident in a timely manner.
 - a. Reporting Requirements. Upon discovery of a privacy incident, the following shall occur:
 - (1) Personnel report the incident to their Commanding Officer.
 - (2) The Commanding Officer, in conjunction with the local Information Systems Security Officer (ISSO) and District/Area legal office, reports by telephone, fax, or email, via enclosure (1) to:
 - (a) The Coast Guard Computer Incident Response Team (CGCIRT), who in turns notifies Commandant (CG-611).
 - (b) Commandant (CG-611) notifies Commandant (CG-6), the DHS Privacy Office, and Commandant (CG-861).

Note: Notify the Coast Guard Investigative Service and the appropriate police/federal law enforcement agencies if theft or other illegal activity is suspected.

- b. CGCIRT Responsibilities. CGCIRT shall forward all reports of a suspected or confirmed privacy incident to the DHS Security Operations Center (DHS-SOC), which reports to the US-CERT.
- c. Notification Requirements. Notification provides impacted individuals the opportunity to take steps to help protect themselves from the consequences of a privacy incident. This notification is also consistent with the “disclosure principle” of reference (a) that requires agencies to inform individuals about how their information is being accessed and used, and may help individuals mitigate potential harm resulting from a privacy incident. Commanding Officers shall determine within 48 hours of being advised of a privacy incident whether notification of impacted individuals is required.
 - (1) Commanding Officers shall assess the likely risk of harm caused by the privacy incident and then assess the level of risk by considering a wide range of harms, such as damage to reputation and the potential for harassment or prejudice—particularly when health or financial information is involved. Notification when there is little or no risk of harm might create unnecessary concern and confusion. If the Commanding Officer is unsure

what type of notification is appropriate, he/she should contact his/her servicing legal office and/or Commandant (CG-61) for advice.

- (2) Enclosure (2) provides privacy incident notification considerations and guidance. The notification must explain the circumstances surrounding the incident, indicate if access to one year of free credit reports/access to identity theft counseling is being offered, and detail the remedial action taken. Note: The Commanding Officer is responsible for determining if provision of free credit reports/identity counseling is appropriate. Provision of these services is particularly appropriate in incidents involving social security numbers, PINs, financial account numbers, or medical data. The **unit shall incur the cost** of providing free credit reports/identity theft counseling. Commanding Officers should seek guidance from the local Contracting Officer to arrange for these services.
 - (3) A press release or a website may be warranted. Seek guidance from public affairs personnel and notify Commandant (CG-61) prior to issuing a public announcement. Enclosure (3) contains details on establishing a call center that provides those affected by the privacy incident an opportunity to obtain additional information regarding the incident.
 - (4) Within 10 days from the date of the incident, submit a report to Commandant (CG-61) detailing remedial action taken, initiatives to reduce risk of harm, any additional processes established to mitigate future incidents, overall impact to the Coast Guard, and the final resolution.
9. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this Instruction and have been determined non-applicable.
10. FORMS/REPORTS. Enclosure (1), Privacy Incident Report, of this Instruction is available in the USCG Electronic Forms library on the Standard Workstation, on the Internet at: <http://www.uscg.mil/forms/>, on the Intranet at <http://cgweb2.comdt.uscg.mil/CGFORMS/Welcome.htm>, and on CG Central at <http://cgcentral.uscg.mil/>.

D. T. GLENN/s/
Assistant Commandant for Command, Control,
Communications, Computers, and Information
Technology

Enclosures: (1) Privacy Incident Report, Form CG-5260A
(2) Privacy Incident Notification
(3) Guidance for Establishing a Call Center

PRIVACY INCIDENT REPORT

Date _____

1. Unit/Command _____
2. POC: _____ (name, title/grade)
3. POC Telephone: _____
4. POC Email Address: _____
5. Date of Incident: _____
6. Number of individuals impacted: _____ actual/estimate (circle one)

- Provide percentage of each of the groups below impacted:

- (1) Active duty _____
- (2) Reserve: _____
- (3) Civilian: _____
- (4) Contractor: _____
- (5) Other: _____ (explain)

7. CGIS Agent (if applicable): _____
 - Telephone number: _____ Email Address: _____
8. CG Attorney: _____
 - Telephone number: _____ Email Address: _____

9. Provide a brief description of the incident, including the circumstances, information lost or compromised, and if the PII was encrypted or password protected. **(DO NOT DISCLOSE ANY PII IN THIS REPORT)**

10. Is the incident suspected or confirmed? _____

11. Explain how the information was compromised or potentially compromised.

12. State the media involved (e.g., paper records, flash drive, mobile device, Intranet, Internet, mail system, email, etc.) and identify to whom information was disclosed (e.g., whether it was disclosed internally (within CG) or externally).

13. Explain remediation measures taken to reduce risk of harm.

14. Describe any additional steps to mitigate future situations.

Privacy Incident Notification

The best means for providing notification will depend on the number of individuals affected and the contact information available about the individuals. Notice provided to individuals affected by a privacy incident should be commensurate with the number of people affected and the urgency with which they need to be notified. The following examples are types of notices which may be considered.

- a. Telephone. Telephone notification may be appropriate in those cases when urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.
- b. First-Class Mail. First-class mail to the last known mailing address of the impacted individual in your agency's records should be the primary means to provide notification. If you have reason to believe the address is no longer current, you should take reasonable steps to update the address by consulting with other agencies, such as the US Postal Service. Send the notice separately from any other documents, so that it is conspicuous to the recipient. If the unit which experienced the privacy incident uses another entity to facilitate mailing (for example, consulting the Internal Revenue Service for current mailing addresses of affected individuals), care should be taken to ensure the unit is identified as the sender, and not the facilitating agency. Label the face of the envelope to alert the recipient to the importance of its contents, *e.g.*, "Privacy Incident Information Enclosed" and include the name of the unit as the sender, to reduce the possibility the recipient may conclude it as advertising mail.
- c. E-Mail. E-mail notification is problematic, because individuals change their e-mail addresses and often do not notify third parties of the change. Notification by postal mail is preferable. However, where an individual has provided an e-mail address to you and has expressly given consent to use as the primary means of communication with your agency, and no known mailing address is available, notification by e-mail may be appropriate. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the privacy incident warrant this approach. E-mail notification may include links to the Coast Guard and www.USA.gov websites, where the notice may be "layered" so the most important summary facts are up front, with additional information provided under linked headings.
- d. Newspapers or other Public Media Outlets. Additionally, you may supplement individual notification by using newspaper ads, websites, or other public media outlets. Contact the local Public Affairs office as indicated in "Procedures," paragraph 8c(3). Enclosure (3) contains guidance for establishing a call center to answer inquiries from affected individuals and the public.

- e. Substitute Notice(s). Post substitute notices in instances when you do not have sufficient contact information to provide direct notification. A substitute notice can consist of a conspicuous posting on the Coast Guard home page website and/or notification to major print and broadcast media, including areas where the affected individuals are believed to reside. Include in the notice, a toll-free phone number where an individual can learn whether or not his or her personal information is/may be included in the privacy incident.

- f. Accommodations. Give special consideration consistent with Section 508 of the Rehabilitation Act of 1973 for providing notice to individuals who are visually or hearing impaired. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the Coast Guard website.

Guidance for Establishing a Call Center

In the event of a privacy incident, the following guidance is provided for determining whether and how to establish a call center to handle inquiries related to the incident. The purpose of a call center is to provide individuals a means for obtaining additional information regarding a privacy incident and possible actions to mitigate an incident's impact on their personal lives (e.g. identify theft, etc.).

- a. The decision to establish a call center should be based on several factors:
 - (1) If a privacy incident does not extend outside the organization (i.e., those affected by the privacy incident are known and can be contacted) the establishment of a call center would normally not be necessary;
 - (2) If a privacy incident affects a large number of individuals and those individuals are not easily identifiable (e.g., "all merchant mariners who were issued an able bodied seaman endorsement since 1975"); establishment of a call center should be considered to allow those potentially impacted to call and obtain additional information regarding the privacy incident.
 - (3) Each situation will be unique and the decision to establish a call center must be based on the circumstances. The main concern should be sharing information with those affected regarding how they can obtain assistance.

- b. If the decision is made to establish a call center, contact your local Contracting Officer to arrange for one of the following services:
 - (1) Obtain a toll-free number (e.g. AT&T, Sprint, Verizon, etc.). The business or government services area of a provider's website can provide information regarding who to contact, features, costs, etc. This option is usually the least expensive, since the unit will be providing its own personnel to answer the phone(s).
 - (2) Implementation of a call center supported and staffed by GSA. This can be accomplished by contacting the General Services Administration's (GSA) USA Services Group. A statement of work (SOW) will be required and the call center can be established within 72 hours thereafter. A generic SOW and the requirements can be found at <http://www.usaservices.gov> under FirstContact. Provide a thorough description of the incident and a list of frequently asked questions for GSA personnel to use when fielding questions. Contact the GSA Contracting Office at 202-501-1797 for additional details.

- c. Items to consider based on the nature of the privacy incident would include, but are not limited to:
 - (1) Use of unit personnel to manage/oversee the call center.

- (2) Training of call center operators.
- (3) Ability to adjust manning in response to call volume.
- (4) Daily hours of operation.
- (5) Cost of service.
- (6) Logging calls.
- (7) Advertising call center number(s) and making privacy incident information readily available to those affected (i.e., on command's and other appropriate websites, mass e-mailing(s), news media, etc.).
- (8) Monitoring call center to ensure quality customer service.
- (9) Criteria for dissolving the call center.
- (10) Pre-staged frequently asked questions (FAQs). These should be reviewed by your servicing legal office. Below are questions which could be used as a benchmark and tailored to meet the requirements of a specific privacy incident.

d. Samples of Frequently Asked Questions:

- (1) How can I tell if my information has been compromised?

At this point, there is no evidence that any missing data has been used illegally. However, the Coast Guard is asking each individual to be extra vigilant and to carefully monitor bank, credit card, and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved.

- (2) What is the earliest date at which suspicious activity might have occurred due to this data privacy incident?

The information was stolen/lost on or about _____(date). If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely affected individuals may notice suspicious activity during the month of _____.

- (3) I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?

The Coast Guard strongly recommends individuals closely monitor their financial statements and visit the Coast Guard's special website at www._____.

(4) Where should I report suspicious or unusual activity?

The Federal Trade Commission (FTC) recommends the following four steps if you detect suspicious activity:

Step 1 – Contact the fraud department of any one of the three major credit bureaus:

- Equifax: 1-800-525-6285; www.equifax.com;
P.O. Box 740241, Atlanta, GA 30374
- Experian: 1-888-EXPERIAN (397-3742); www.experian.com;
P.O. Box 9532, Allen, TX 75013
- TransUnion: 1-800-680-7289; www.transunion.com;
Fraud Victim Assistance Division
P.O. Box 6790, Fullerton, CA 92834

Step 2 – Close any accounts that have been tampered with or opened fraudulently.

Step 3 – File a police report with your local police or the police in the community where the identity theft occurred.

Step 4 – File a complaint with the FTC by using its Identity Theft Hotline: 1-877-438-4338, online at www.consumer.gov/idtheft, or by mail at:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue NW,
Washington, DC 20580.

(5) I know the Coast Guard maintains my _____ records electronically. Was this information compromised?

No _____ records were compromised. The data lost is primarily limited to an individual's name, e-mail address and home phone number. However, this information could still be of potential use to identity thieves and we recommend vigilance in monitoring for signs of potential identity theft or misuse of their information.

(6) Where can I receive updated information?

The Coast Guard has set-up a special website and a toll-free telephone number for individuals with up-to-date news/information. Please visit www.uscg.mil or call 1-800-XXX-XXXX.

(7) Does the electronic data theft affect only _____?

It may potentially affect _____ as well.