

R 291947Z AUG 07 ZUI ASN-A00241000008 ZYB
FM COMDT COGARD WASHINGTON DC//CG-6//
TO ALCOAST

BT

UNCLAS //N05215//

ALCOAST 425/07

COMDTNOTE 5720

SUBJ: SAFEGUARDING PERSONAL PRIVACY INFORMATION

A. OMB MEMO OF 12 JUL 06 ON REPORTING INCIDENTS INVOLVING
PERSONALLY IDENTIFIABLE INFORMATION (PII), OMB M-06-19

B. COAST GUARD FREEDOM OF INFORMATION (FOIA) AND PRIVACY ACTS
MANUAL, COMDTINST M5260.3

C. COAST GUARD PRIVACY IMPACT ASSESSMENT (PIA), COMDTINST 5260.4
(SERIES)

D. OMB MEMO OF 22 MAY 07 ON SAFEGUARDING AGAINST AND RESPONDING TO
THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII), OMB M-07-
16

E. THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

1. THIS ALCOAST PROVIDES INFORMATION REGARDING PII IN ADVANCE OF A
FORTHCOMING INSTRUCTION. IN LIGHT OF INCREASED MEDIA EXPOSURE AND
PUBLIC SCRUTINY OF A NUMBER OF FEDERAL AGENCY BREACHES, I
REEMPHASIZE THE IMPORTANCE OF PROTECTING PII HELD BY THE COAST
GUARD (CG) AND CHALLENGE COMMANDING OFFICERS TO REVISE BUSINESS
PROCESSES WHEREVER POSSIBLE TO MINIMIZE OR ELIMINATE THE COLLECTION
AND USE OF PERSONAL INFORMATION, AND TO USE THE EMPLID INSTEAD OF
PARTIAL OR FULL SSNS WHENEVER POSSIBLE.

2. THE CG MAINTAINS A SIGNIFICANT AMOUNT OF INFORMATION CONCERNING
INDIVIDUALS AND HAS A SPECIAL DUTY TO PROTECT PII FROM DISCLOSURE,
LOSS, OR MISUSE.

3. PII IS DEFINED BY REFERENCE A AS "ANY INFORMATION ABOUT AN
INDIVIDUAL MAINTAINED BY AN AGENCY, INCLUDING, BUT NOT LIMITED TO,
EDUCATION, FINANCIAL TRANSACTIONS, MEDICAL HISTORY, CRIMINAL OR
EMPLOYMENT HISTORY, AND INFORMATION WHICH CAN BE USED TO
DISTINGUISH OR TRACE AN INDIVIDUALS IDENTITY, SUCH AS THEIR NAME,
SOCIAL SECURITY NUMBER (SSN), DATE AND PLACE OF BIRTH, MOTHERS
MAIDEN NAME, BIOMETRIC RECORDS, ETC., INCLUDING ANY OTHER PERSONAL
INFORMATION WHICH IS LINKED OR LINKABLE TO AN INDIVIDUAL." THE
LOSS OF PII CAN RESULT IN SUBSTANTIAL HARM, EMBARRASSMENT, AND
INCONVENIENCE TO INDIVIDUALS AND MAY LEAD TO IDENTITY THEFT OR
OTHER FRAUDULENT USE OF INFORMATION.

4. THE PRIVACY ACT REQUIRES THAT INFORMATION WHICH CAN BE
ACCESSED BY PERSONAL IDENTIFIERS RECEIVES PARTICULAR PROTECTIONS.
ALL SYSTEMS COLLECTING SUCH INFORMATION MUST HAVE A SYSTEM OF
RECORDS NOTICE (SORN) PUBLISHED IN THE FEDERAL REGISTER. THE SORN
ESTABLISHES WHAT INFORMATION IS BEING COLLECTED, THE PURPOSE FOR
THE COLLECTION, WHO MAY ACCESS THE INFORMATION, AND THE
CIRCUMSTANCES WHEN THE INFORMATION CAN BE SHARED. SYSTEM MANAGERS
ARE RESPONSIBLE FOR ENSURING PROVISIONS IN THEIR RESPECTIVE SORNS
ARE FOLLOWED. THE CGS POLICIES FOR MANAGING SORNS ARE PROMULGATED
IN REFERENCES B AND C.

5. THE PRIVACY ACT ALSO STATES EACH AGENCY MUST ESTABLISH
APPROPRIATE ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS TO
ENSURE THE SECURITY AND CONFIDENTIALITY OF RECORDS AND TO PROTECT
AGAINST ANY ANTICIPATED THREATS OR HAZARDS TO THEIR SECURITY OR
INTEGRITY WHICH COULD RESULT IN SUBSTANTIAL HARM, EMBARRASSMENT,
INCONVENIENCE, OR UNFAIRNESS TO ANY INDIVIDUAL ON WHOM INFORMATION
IS MAINTAINED.

6. REFERENCE D REQUIRES ALL AGENCIES TO REPORT SECURITY INCIDENTS
TO THE FEDERAL INCIDENT RESPONSE CENTER, UNITED STATES COMPUTER
EMERGENCY READINESS TEAM (US-CERT) WITHIN ONE HOUR OF DISCOVERY.

REFERENCE A HAS REVISED THOSE REPORTING PROCEDURES TO NOW REQUIRE AGENCIES TO REPORT ALL PRIVACY INCIDENTS INVOLVING PII, IN ELECTRONIC OR PHYSICAL FORM, REGARDLESS OF WHETHER THE INCIDENT IS MERELY SUSPECTED OR HAS BEEN CONFIRMED, TO US-CERT WITHIN ONE HOUR OF DISCOVERY.

7. CG PERSONNEL SHALL REPORT ALL PRIVACY INCIDENTS, WHETHER IN ELECTRONIC OR PHYSICAL FORM, TO THE COMMANDING OFFICER UPON DISCOVERY--REGARDLESS OF WHETHER THE INCIDENT IS MERELY SUSPECTED OR HAS BEEN CONFIRMED. THIS REPORTING REQUIREMENT APPLIES TO ALL CG PERSONNEL--INCLUDING ACTIVE DUTY, RESERVE, CIVILIAN EMPLOYEES, INDEPENDENT CONSULTANTS, AND GOVERNMENT CONTRACTORS WHO USE, OR HAVE ACCESS, TO CG INFORMATION RESOURCES. THE COMMANDING OFFICER SHALL NOTIFY THE CG COMPUTER INCIDENT RESPONSE TEAM (CGCIRT) AT (800)4CG-CIRT/(800)424-2478. CGCIRT SHALL NOTIFY BOTH THE ASSISTANT COMMANDANT FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INFORMATION TECHNOLOGY (CG-6), AS WELL AS THE OFFICE OF INFORMATION MANAGEMENT (CG-61), PRIOR TO BRIEFING THE US-CERT.

8. COMMANDING OFFICERS REMAIN RESPONSIBLE FOR SAFEGUARDING PII, AS WELL AS DEVELOPING AND IMPLEMENTING A REPORTING PLAN FOR THEIR AREA OF RESPONSIBILITY (AOR) TO COMPLY WITH REFERENCE E AND THE ONE HOUR REPORTING REQUIREMENT OUTLINED IN REFERENCE A. COMMANDING OFFICERS SHOULD REVIEW THEIR CURRENT STANDARD OPERATING PROCEDURES (SOP) TO ENSURE THEY ARE EXERCISING ADEQUATE SAFEGUARDS TO PREVENT INTENTIONAL OR NEGLIGENT MISUSE OF, OR UNAUTHORIZED ACCESS TO PII. THIS REVIEW SHOULD INCLUDE ALL ADMINISTRATIVE, TECHNICAL, AND PHYSICAL MEANS USED TO CONTROL SUCH INFORMATION--INCLUDING, BUT NOT LIMITED TO, PROCEDURES AND RESTRICTIONS ON USE OR REMOVAL OF PII BEYOND AGENCY PREMISES OR CONTROL.

9. SYSTEM MANAGERS AND ALL OTHERS WHO COLLECT, MAINTAIN, AND DISSEMINATE PII SHALL REVIEW THE PRIVACY PORTION OF THE FREEDOM OF INFORMATION ACT/PRIVACY ACT TUTORIAL AT [HTTP://WWW.USCG.MIL/CCS/CIT/CIM/FOIA/FOIAPATUTORIAL/](http://www.uscg.mil/ccs/cit/cim/foia/foiapatutorial/)

10. PROMULGATION OF AN INSTRUCTION FOR SAFEGUARDING PERSONAL PRIVACY INFORMATION AND BREACH NOTIFICATION REQUIREMENTS IS FORTHCOMING AS NOTED ABOVE.

11. POC IS DONALD TAYLOR, 202-475-3519, EMAIL DONALD.G.TAYLOR(AT)USCG.MIL.

12. INTERNET RELEASE AUTHORIZED.

13. RELEASED BY RDML D.T. GLENN, ASSISTANT COMMANDANT FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INFORMATION TECHNOLOGY.

BT

NNNN

Protecting & Handling Personnel-Related Data – Quick Reference Guide

Do make sure all personnel-related data is marked “For Official Use Only” or “Privacy Data.”

Do protect personnel-related data according to the privacy and security safeguarding policies.

Do report any unauthorized disclosures of personnel-related data to your supervisor, Program Manager, or Information System Security Manager.

Do immediately report any suspected security violation or poor security practices relating to personnel-related data.

Do lock up all notes, documents, removable media, laptops, and other material containing personnel-related data when not in use and/or under the control of a person with a need to know.

Do log off, turn off, or lock your computer whenever you leave your desk to ensure that no personnel-related data is compromised.

Do encrypt all personnel-related data documents sent via e-mail.

Do destroy all personnel-related data in your possession when no longer needed and continued retention is not required.

Do be conscious of your surroundings when discussing personnel-related data. Protect verbal communication with the same heightened awareness as you would paper or electronic personnel-related data.

Don't leave personnel-related data unattended. Secure it in a locked drawer, locked file cabinet, or similar locking enclosure, or in a room or area where access is controlled and limited to persons with a need to know.

Don't take personnel-related data home, in either paper or electronic format, without written permission of your supervisors, office chief, or Information Security Systems Manager, as required.

Don't discuss or entrust personnel-related data to individuals who do not have a need to know.

Don't discuss personnel-related data on wireless or cordless phones unless absolutely necessary. Unlike landline phones, these phones can be more easily intercepted.

Don't put personnel-related data in the body of an e-mail. It must be password-protected as an attachment.

Don't dispose of personnel related data in recycling bins or regular trash unless it has first been shredded.