DEPARTMENT OF HOMELAND SECURITY

U.S. Coast Guard

PRIVACY INCIDENT REPORT

Privacy Act Statement

Authority: 5 U.S.C 552a(e)(9)-(10); 44 U.S.C. 3534

Purpose: United States Coast Guard (USCG) personnel will utilize this form to document any suspected or confirmed privacy incident.

Routine Uses: Authorized Coast Guard personnel will use this form to assess the severity of any suspected or confirmed privacy incident and initiate remediation efforts. Any external disclosures of data within this record will be made in accordance with DHS/ALL-004, Department of Homeland Security General Information Technology Access Account Records, 77 Federal Register 70792, November 27, 2012.

Disclosure: Furnishing this information is voluntary; however, failure to furnish the requested information may impede remediation efforts.

1. Unit/Command

2. POC *(Name Title/Grade)*	3. POC Telephone	4. Date of Incident

5. CO's *(Name/Signature)**	**Signature responsibility may "only" be delegated to the Executive Officer (XO) or acting XO.*	6. Date

7. Number of individuals impacted: _____actual/estimate *(check one)*

Provide percentage of each of the groups below impacted:

Active duty: _____ Civilian: _____

Reserve: _____ Contractor: _____

Other: _____ *(explain)*

_____

8. PII Data Elements Exposed *(check all that apply)*

- ☐ Full Name
- ☐ SSN
- ☐ EMPLID
- ☐ Date of Birth
- ☐ Home Address
- ☐ Commercial Email Address
- ☐ Other *(if not listed)*
- ☐ Telephone Number
- ☐ Financial Info
- ☐ Medical Info
- ☐ Performance Rating
- ☐ Drivers License Number
- ☐ Passport Number
- ☐ Credit Card Number

_____

7. CGIS Agent (*if applicable)*	Telephone Number	Email Address
8. CG Attorney	Telephone Number	Email Address

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

12. Is the incident suspected or confirmed?

13. Explain how the information was compromised or potentially compromised. *(DO NOT LIST RESPONSIBLE INDIVIDUAL'S NAME)*

14. 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).*

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

16. Describe any additional steps to mitigate future situations.

Reset