



Privacy Impact Assessment
for the
**United States Coast Guard
National Pollution Funds Center**

**Pollution Response Funding, Liability, and
Compensation System (NPFC PRFLACS)**

June 17, 2009

Contact Point

**Amy Casillas-Becker
National Pollution Funds Center (NPFC)
U.S. Coast Guard
(202) 493-6771/ (202) 493-6949**

Reviewing Official

**Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780**



Abstract

The United States Coast Guard (USCG) National Pollution Funds Center's (NPFC) Pollution Response Funding, Liability, and Compensation System (PRFLACS) support the command's mission to administer the financial responsibility provisions in Title I of the Oil Pollution Act. The purpose of this Privacy Impact Assessment (PIA) is to ensure that adequate privacy considerations and protections continue to be applied to the personally identifiable information (PII) maintained in the NPFC PRFLACS system.

Introduction

The NPFC's principal mission is to administer the financial responsibility provisions in Title I of the Oil Pollution Act of 1990. NPFC administers the Oil Spill Liability Trust Fund that supports the Oil Pollution Act activities; the Coast Guard portion of the Environmental Protection Agency (EPA) Superfund, which supports the Comprehensive Environmental Response, Compensation, and Liability Act of 1980; and pollution-related disaster funds under the Stafford Act and the National Response Plan. These laws deal with liability, compensation, and other fiscal matters stemming from threatened or actual oil or hazardous substance releases.

NPFC Pollution Response Funding, Liability, and Compensation System (PRFLACS) Functions

The NPFC PRFLACS includes five non- major systems that collectively comprise NPFC's overarching mission support system. The five NPFC systems are:

- Case Information Management System (CIMS)
- Ceiling and Number Assignment Processing System (CANAPS)
- Claims Processing System (CPS)
- Certificate of Financial Responsibility (COFR)
- Electronic Certificate of Financial Responsibility (e-COFR)

Case Information Management System

The purpose of the Case Information Management System is to support the NPFC's mission to manage the funding and prosecution of pollution incident cases. The Case Information Management System is a mixed financial system (approximately 30% financial and 70% case management information) that receives obligation and expenditure downloads from USCG's Core Accounting System (CAS). The system includes both financial and non-financial information about pollution incident response cases, case team members, response costs, incident responsible parties, and cost recovery efforts. It includes PII about responsible parties. A user interface allows for direct entry and update of case information.



Ceiling and Number Processing System

The Ceiling and Number Assignment and Processing System is a front end module to the Case Information Management System that provides an automated method for the assignment of a Federal Project Number or Comprehensive Environment Response, Compensation, and Liability Act of 1980 Project Number for an oil spill or hazardous material (hazmat) release. USCG and EPA Federal On-Scene Coordinators require access to Oil Spill Liability Trust Fund or the Comprehensive Environment Response, Compensation, and Liability Act of 1980 funds to respond to pollution incidents. The Ceiling and Number Processing System also automatically generates and issues a notification message providing budget amount, project number and accounting string, to key parties via the Coast Guard Messaging System (USCGMS).

Claims Processing System

NPFC's Claims Processing System supports the NPFC mission to adjudicate and pay third party claims for damages resulting from oil pollution incidents. It also supports claims from trustees for Natural Resource Damage assessments and restoration.

The Claims Processing System is a work flow system that supports the initial receipt, administrative processing, and subsequent routing and payment of claims through NPFC. The primary input mechanism for the Claims Processing System is the user interface, which provides the means to capture user information, perform edits, and process the information. It interfaces with the Case Information Management System to ensure associated cases exist for submitted claims. This system includes information about the claimants and responsible parties.

If an individual or organization suffers certain damages or incurs removal costs because of a discharge or a substantial threat of a discharge of oil to U.S. navigable waters, the Oil Pollution Act entitles them to seek compensation from the Oil Spill Liability Trust Fund. Claims not paid by the incident's responsible party or resulting from mystery spills for which a responsible party cannot be identified may be submitted to the NPFC for payment.

Certificate of Financial Responsibility System

Certificates of Financial Responsibility (COFRs) are used to manage access to U.S. waters and identify responsible parties for covering costs associated with any related pollution incidents. The Certificate of Financial Responsibility System tracks and manages COFR applications, active COFRs and their related vessels, operators, and guarantors required to demonstrate they have sufficient funds to meet the maximum amount of liability to which they could be subjected. The primary input mechanism for the Certificate of Financial Responsibility System is the User Interface, which captures user information, performs edits, and processes the information. Active COFRs push data from the Certificate of Financial Responsibility System to Electronic Certificate of Financial Responsibility System for the active COFR Search capability. The Certificate of Financial Responsibility System also accepts and processes COFR search queries from Marine Information for Safety Law Enforcement (MISLE).



Electronic Certificate of Financial Responsibility System

The Electronic Certificate of Financial Responsibility (e-COFR) System is a front-end web application for the Certificate of Financial Responsibility System. The e-COFR System resides on the Internet and the maritime industry uses the system to submit COFR applications and pay associated processing fees. PAY.GOV receives and processes all payments. No payment information is captured or stored by e-COFR.

Typical Transaction

Maritime Operators must submit vessel COFR applications to apply for or renew a certificate via the NPFC Insurance Examiner using the e-COFR system and pay the associated filing fee. The NPFC Insurance Examiner approves the COFR application once it is received and enters the information into the internal COFR system. An automatic interface synchronizes COFR certificate status data between COFR and e-COFR, to assure data integrity and validation.

Port Operations verifies the COFR status of vessels requesting access to U.S. navigable waters, by querying e-COFR or through the MISLE-to-COFR query to allow the vessel passage. In the event of a pollution incident (releasing oil in U.S. waterway) involving a valid COFR vessel in U.S. navigable waters, the COFR vessel notifies the National Response Center (NRC) and the local USCG unit of the incident. The USCG unit opens a pollution response project and requests funding via CANAPS.

CANAPS processes the request, issues a project number, and authorizes response funding (aka "Ceiling"). The CANAPS application interfaces with the CIMS application to open the project record and assigns a projected cost budget. CIMS generates an email notice to Finance Center (FINCEN) to open the project and budget in their USCG Core Accounting System (CAS). The USCG unit coordinates pollution response and records response obligations and expenditures in CAS, which are downloaded nightly into CIMS. The NPFC Case Officer oversees pollution response spending and updates project status in CIMS. All NPFC project correspondences are generated and stored in the CIMS application.

If an injured third party submits a claim for damages (e.g., lost profits) from the pollution incident, it is routed through the NPFC Claims Manager. The NPFC Claims Manager receives the claim and enters claim information into the Claims Processing System (CPS) application. A CPS-to-CIMS interface associates the claim with the relevant project in CIMS. The NPFC Claims Manager adjudicates the claim and updates claim status in CPS. If payment is due on claim, the NPFC Claims Supervisor approves the claim payment in CPS. The CPS application then generates Authorization to Pay (ATP) memorandum that NPFC submits to FINCEN for processing. Claim payment information is downloaded from CAS to CIMS and CPS. The NPFC Case Officer uses CIMS to bill the incident's Responsible Party. All incident payments are recorded in CIMS. Then the claim and the Pollution Response Project are closed.

These systems throughout the remainder of the PIA will be referred to as the NPFC Pollution Response Funding, Liability, and Compensation System.



System Information Use and Collection

NPFC PRFLACS consists of information relating to the funding, liability, and management of pollution incident response and recovery costs from responsible parties. Information in the system varies from incident location and claimant information to case officer and payment information.

NPFC PRFLACS shares information with several government organizations internal and external to DHS. The sharing of information in pursuant to the routine sharing requirements at established in the Department of Homeland Security Accounts Payable System of Records DHS/ALL-007 (October 17, 2008, 73 FR 61880) and the Department of Homeland Security Accounts Receivable System of Records DHS/ALL-008 (October 17, 2008, 73 FR 61885) The amount of PII shared is limited.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

NPFC PRFLACS consists of information relating to the liability, funding and management of pollution incident responses and recovery of costs from responsible parties. The collection of paper and electronic submissions from USCG and other government personnel, as well as from external sources, such as incident responsible parties and claimants, become part of NPFC's records. The information in the system is primarily organized by pollution project; however, it does contain information on responsible parties, some of whom are individuals, and on the government personnel involved in managing the case. Usually, system users retrieve data by project number; but, occasionally, they may also search for responsible parties, claimants, vessel owners/operators/guarantors, or employees by name.

NPFC PRFLACS collects the following information:

- Contact information may include some or all of the following: full name, home address, email address, and home telephone number, work telephone number, work mailing address, work email address, date of birth, taxpayer identification number, financial/tax information, social security number;
- Authorized budget, obligations, expenditures, and cost recovery information;
- Case status information such as whether it is an active pollution response or if cleanup is complete;
- Spill information including incident name, date, location, state, and body of water;
- Claim information including type, amount, description, explanation, and electronic documents associated with the claim (correspondence to and from the claimants or their representative);



- COFR information including, applicant name, address, state or country where incorporated, fees paid, COFR number, and status;
- Vessel information including name, type, size, country of registration, owner information (name and address), guarantor information (name and address);
- Business contact information including name and address on certain individuals (point of contact, company official, agent, etc.) who are employed by or associated with a vessel operator; and
- NPFC Marine Examiner processing the COFR information including name and examiner number.

If NPFC approves a claim for payment, a Social Security number (SSN) or Tax Identification number (TIN) is collected from the claimant.

1.2 From whom is information collected?

NPFC may collect information from the following:

- Federal On-Scene Coordinators and other government participants in spill response;
- Responsible parties (companies and individual persons);
- Claimants;
- Other interested parties such as agents, attorneys, or subject matter specialists;
- USCG and other government financial systems;
- Research by NPFC personnel and contractors for cost recovery;
- Individual including witnesses and other third parties;
- Corporations, partnerships, or associations;
- United States government;
- Federal, state, foreign, or Indian tribe trustee;
- States, the District of Columbia, municipalities, and political subdivisions of States;
- Commonwealth of Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Commonwealth of the Northern Marianas Islands, and any other territory or possession of the United States;
- Certain foreign claimants;
- Information is collected from the vessel operators applying for the COFRs. Only "operators" as defined in 33 CFR 138.20(b) may apply for COFRs.



1.3 Why is the information being collected?

NPFC needs certain information in order to manage the use of the fund and recover appropriate costs. Responsible party identifying information is needed to establish liability and prosecute cost recovery. Additionally, if individuals or organizations suffer loss of damage due to an oil spill, the Oil Pollution Act entitles them to seek compensation. Indeed, fair compensation is an important aspect of final recovery from the spill. The NPFC has the authority to use the Oil Spill Liability Trust Fund to pay for uncompensated removal costs and damages. The NPFC uses the information collected to adjudicate the claim.

With a few limited exceptions, vessels greater than 300 gross tons and vessels of any size that are lightering or transshipping oil in the Exclusive Economic Zone (EEZ) must comply with the COFR regulations in order to operate in U.S. waters. Failure to submit required information will prevent the issuance of the COFR, and the vessel will not be permitted to operate in U.S. waters.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

NPFC legal authorities include several laws:

- Clean Water Act [33 USC 1251-1387]
- Oil Pollution Act of 1990 (OPA) [26 USC 9509; 33 USC 2761]
- Debt Collection Act of 1982 [15 USC 1692]
- Internal Revenue Code Identifying Numbers [26 USC 6109]
- Money and Finance: Collection and Compromise of Claims of the US Government [31 USC 3711]
- Financial Responsibility for Water Pollution (Vessels) [33 CFR 138]
- Title VI of the Coast Guard and Maritime Transportation Act of 2006 (Delaware River Protection Act of 2006) [Public Law 109-241]
- Chief Financial Officers (CFO) Act [Public Law 101-576]

1.5 **Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.**

While the collection of some information in NPFC PRFLACS represents a privacy risk, NPFC minimizes the amount of information it collects to only that needed to perform its mission, and restricts its use to those with a valid need-to-know.



Access to the electronic records is restricted to those with specific roles in the case management and claims adjudication processes. User accounts are role-based with privileges designed for need-to-know. Audit trails are maintained and reviewed to identify unauthorized access. Personnel complete training on their business roles as well as how to use and protect electronic information. Computer security training is mandatory to be completed on an annual basis

The management, technical, and operational controls are reviewed every three years or less as part of the system certification and accreditation process.

Protection of NPFC PRFLACS is through an extensive firewall capability provided by the USCG Telecommunications and Information Systems Command. Data storage media are housed behind barriers with card key lock protection. Data storage media are scrubbed prior to disposal in accordance with established NIST guidelines.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

Uses of information include:

- Case status tracking and reporting, including information on the case and responsible parties to spill responders to aid in investigations and response and to the general public for information on submitting claims;
- Response funding (project initiation, budget authorization, obligation/expenditure management);
- Cost recovery functions, including possible referral to Debt Management Services in the Department of the Treasury or to the Department of Justice for litigation;
- Claim status tracking and reporting, including information on the claimant and responsible parties to aid with the evaluation and adjudication;
- Claim adjudication, including the possible coordination with Federal Trustees;
- Issuing COFRs to vessel operators who have demonstrated adequate evidence of financial responsibility as established by law;
- Responding to compliance inquiries from USCG and Customs and Border Protection field offices and from the Louisiana Offshore Oil Port to ensure that all vessels that require COFRs have them;
- Funds management and status reporting;
- Responses to Congressional inquiries; and
- FOIA and Privacy Act requests.



2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as “datamining”)?

The system does not conduct datamining. Data analysis monitors trends (e.g., in quantity and size of cases) and help assess business process effectiveness.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Multiple stages throughout the life cycle of the data check for accuracy. Data edits, integrity rules, and error traps are performed during data capture and update processes. Primary communications with the responsible parties are via certified mail.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The information assists NPFC’s statutory requirements to manage pollution response funding and perform cost recovery. Technical security and access measures are in place to ensure user authorization to access NPFC. As part of the standard operating procedures, NPFC personnel perform numerous attempts to communicate with responsible parties and applicants to inform them of their status and to encourage them to correct erroneous information.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

The NPFC is currently working with NARA to develop retention schedules for both the paper and electronic data. We anticipate that the data on certain “significant cases”, such as the T/B Morris J. Berman-074028 and T/V ATHOS I – P05005, may ultimately become permanent and that the retention period for the remaining cases will be a matter of decades (EPA maintains its Superfund cases for 30 years). Until these schedules are completed, the NPFC will transfer the paper files to the Federal Records Center (FRC) when cases are closed and will maintain the electronic data. In addition, paper Certificate of Financial Responsibility files are kept for 10 years after the Certificate of Financial Responsibility expires.



3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

No. A NPFC records retention schedule is under development in cooperation with NARA.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

While many cases are short-lived, others can remain open or be re-opened for many years due to statutes of limitations, litigation, etc. For example:

- The statute of limitations for a removal claim on a pollution incident extends for up to six years after clean-up is completed.
- The statute of limitations for a damage claim on a pollution incident extends for up to three years of the date the damage was reasonably discoverable, which could be significantly later than the clean-up completion date.
- Cases referred to the U.S. Treasury Department's Debt Management Service/Treasury Offset Program can stay in debt collection status for up to ten years.
- Cases referred to the Department of Justice for potential litigation can have an indefinite life.
- Environmental records are generally maintained for longer periods of time than similar non-environmental records.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

Internal organizations share very little information on individuals; most shared information concerns case funding status:

- USCG Legal Directorate – litigation referrals
- Federal On-Scene Coordinators and field units – information requested for investigations and spill response
- USCG Headquarters – mission performance information;
- Districts and Sectors – project status and funding information;
- Finance Center (FINCEN) – project funding authorizations, invoice payment approvals; and
- Maintenance and Logistics Command (MLC) – project funding authorizations; and



- USCG and Customs and Border Protection (CBP) field offices.

4.2 For each organization, what information is shared and for what purpose?

With the exception of litigation referrals and inquiries into specific cases, generally most shared information is aggregate reports from the system; internal organizations do not have direct access to the system:

- Summary financial information (e.g., weekly Oil Spill Liability Trust Fund report);
- Cost recovery status information (weekly AR report, Quarterly Treasury Report on Receivables);
- Project initiation/status information (e.g., Project Ceiling Authorization Notices, FINCEN R06 table updates); and
- Case referrals (reviewed by USCG Legal Directorate) before being referred to the U.S. Department of Justice; and
- The NPFC shares Certificates of Financial Responsibility information with USCG and CBP field offices who are requesting whether a particular vessel has a valid COFR; if the vessel does not have a valid COFR; it is not permitted in U.S. waters.

4.3 How is the information transmitted or disclosed?

Information is transmitted via:

- Email;
- System-generated electronic reports;
- System-generated hardcopy reports;
- Data extracts to MS-Excel and/or MS-Word;
- USCG Messaging System;
- Fax; and
- File copies on CD.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Other internal organizations generally receive a summary level of information, which does not contain personally identifiable information. Legal referrals are appropriately marked for handling of unclassified but sensitive, legally-privileged information.



Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

The following external organizations share our information:

- Contractors for system maintenance or cost recovery;
- U.S. EPA and other spill responders;
- Debt Management Services DMS, U.S. Department of Treasury;
- Internal Revenue Service, U.S. Department of Treasury;
- U.S. Department of Justice (DOJ);
- Courts and adjudicative bodies;
- Government Accountability Office;
- U.S. Congress;
- Louisiana Offshore Oil Port;
- FRC/NARA; and
- News media/general public.

5.2 What information is shared and for what purpose?

Information shared is:

- EPA project initiation/status information;
- Summary financial data, for funds management and status reporting purposes;
- Debt collection information, for debt collection, funds management, and status reporting purposes;
- Legal referral information, for legal support for cost recovery and debt management purposes;
- Case information, especially financial data, in response to a GAO audit request;
- Case files sent to FRC/NARA for archival;
- Whether a particular vessel has a valid COFR; if the vessel does not have a valid COFR, it is not permitted in U.S. waters;
- Summary case information in response to public inquiry; and
- Case documents (often with redacted information) in response to a FOIA, Privacy Act, or Congressional request.



5.3 How is the information transmitted or disclosed?

Information is transmitted via:

- Email;
- System-generated electronic reports;
- System-generated hardcopy reports;
- Data extracts to MS-Excel and/or MS-Word;
- IRS Form 1099-C when an RP's debt is cancelled;
- Direct data entry (e.g., for debt referrals to the U.S. Treasury Debt Management Service);
- Fax; and
- File copies on CD.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

The information shared with the Department of the Treasury's Debt Management Service by the MOU between DHS and Treasury's Financial Management Service, which requires compliance with the Privacy Act.

The NPFC's contracts contain several restrictions dealing with privacy, including signature of DHS Form 11000-6 (Non-Disclosure Agreement), undergoing a security briefing, and/or immediate forwarding of all requests for data outside the contracted function to the NPFC Contracting Officer Technical Representative (COTR).

5.5 How is the shared information secured by the recipient?

In most cases, the NPFC redacts any sensitive information before sending it outside the agency. Only Treasury/DMS, Treasury/IRS, DOJ, the Courts, and FRC/NARA might receive information that must be secured; DMS contracts and federal regulations govern these functions. Contractors for system development and maintenance work within the NPFC offices and are constrained by the same safeguards and security measures as NPFC employees, which are IT Security and PII Security Training, Non-Disclosure Agreements, Background Checks, and System/Personnel Compliance Monitoring.



5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

The DMS contract requires compliance with the Privacy Act as amended, which stipulates training for everyone associated with the system.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

One of the first steps in the NPFC case, claim or certification process is notification to responsible parties, claimants, and applicants, of which a primary purpose is to encourage the correction of erroneous information. Legal referrals are appropriately marked for handling of unclassified but sensitive, legally-privileged information. The Department of Justice, court or adjudicative body receives privacy information only when the identified person(s) is party to legal process and the records are relevant and necessary. The Department of Treasury receives privacy information directly necessary for collection of delinquent debts. Closed case files are marked as Privacy Act files when they are transferred to the FRC for archival purposes in accordance with FRC/NARA procedures.

The NPFC collects privacy information only when and from whom necessary; for instance, instead of requesting Social Security numbers from all individual claimants, claims managers request the information (required for payment under 31 USC 3325) only from claimant whose claims they have approved for payment.

Congress receives information only in response to a direct inquiry from a Congressional office regarding a constituent. Consistent with the Freedom of Information (FOIA) standards, only factual information in the public interest that does not constitute an unwarranted violation of personal privacy is provided to Congress, the news media, and the general public.



Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The NPFC is in the process of submitting a System of Records Notice. In addition, responsible parties receive several notifications of collection throughout the cost recovery process. When a spill occurs, the field provides all known concerned parties a Notice of Federal Interest, which informs them that they may be responsible parties; under the authority of Oil Pollution Act, the field collects information on the responsible parties and forwards it to the NPFC. After reviewing the information, the NPFC then sends responsible parties a notice, which informs them that they are considered liable under Oil Pollution Act, describes potential uses of their information, and encourages them to contact the NPFC to discuss their case information.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

The responsible party, claimant, and applicant can decline to provide information; however, failure to provide requested information may result in negative findings, detainment, denial of entry into U.S. ports, civil penalties, seizure or forfeiture of vessel, or referral of a case for legal proceedings.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

The claim submission form and instructions include a Privacy Act statement. Operators may inform the NPFC of their consent to particular uses when submitting the application. The Debt Collection Act of requires the NPFC to forward unresolved debts to the Department of the Treasury or the Department of Justice for cost recovery.



6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The NPFC is in the process of submitting a System of Records Notice. In addition, whereas it used to wait until response costs were mostly complete before sending a bill and notice of liability; it has changed its procedures to send out the notice early in the process to inform responsible parties that information is being collected and of the possible uses of that information.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Responsible parties, claimants, and applicants may contact the NPFC via hard copy correspondence, email, fax, or telephone to obtain copies of information collected on them.

7.2 What are the procedures for correcting erroneous information?

Responsible parties, claimants, and applicants may contact the NPFC via hard copy correspondence, email, fax, or telephone to correct erroneous information.

7.3 How are individuals notified of the procedures for correcting their information?

The Notice of Potential Liability encourages individuals to contact the assigned NPFC case officer to correct erroneous information. Posted contact information is on the NPFC Internet web site (<http://www.uscg.mil/npfc/>) and on the Ceiling and Number Processing System and e-Certificate of Financial Responsibility applications. Contact information is available on the website so individuals can quickly contact the NPFC if information needs to be corrected.

7.4 If no redress is provided, are alternatives available?

Redress is provided as described in 7.3 above for individuals who believe information on them is incorrect.



7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

The NPFC notifies responsible parties, claimants, and applicants several times of the information we have on them and encourages them to contact the case officer, claims manager or marine examiner if they dispute the information.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

NPFC Case Management, Financial Management, Vessel Management, Claims Management personnel, System Administrators, and Developers have access to NPFC PRFLACS. Roles within the organization, need to know, eligibility, and suitability, determine access privileges. Access privileges must be requested by a supervisor. The NPFC's Information System Security Officer (ISSO) manages and enforces all rules. Other agencies do not have direct access to the system.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes; a contractor supports and maintains NPFC's information technology (IT) systems and provides end-user support. Contractor personnel have access to production data to run ad hoc report and diagnose user problems. All contractor personnel with such access are required to comply with the requirements of the Privacy Act of 1974, as amended, 5U.S.C.§552a. All contractor personnel have completed SF-85P Position of Trust, DHS 11000-6 Non-Disclosure, and USCG AIS 5500.1 forms.

A contractor also provides business and operations support services to the NPFC. Although most of this work is performed offsite, occasionally, some onsite contractors require access to the Case Information Management System. The level of access may vary depending on the support being provided. All contractor personnel with such access are required to comply with the requirements of the Privacy Act of 1974, as amended, 5U.S.C.§552a.

Copies of the contracts are provided separately.



8.3 Does the system use “roles” to assign privileges to users of the system?

Yes. Specific roles in the case management, vessel management, and claims adjudication processes, have access to the electronic records. User accounts are role-based with privileges designed for need-to-know.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Security requirements and user privileges are defined in system requirements documentation. User privilege matrices itemize user groups and their specific members and privileges. NPFC functional and IT management review the tables periodically to confirm that user access remains consistent with assigned responsibilities. NPFC management must approve system access requests for new users.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

System testing addresses all rights and privileges, and verifies that only authorized users can perform specified functions. Applications for system access are reviewed and approved by designated NPFC management personnel.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Systems logs capture information about data transactions such as when an item was changed and by whom. Histories of changes are maintained and read-only copies of completed documents are stored. Audit trails and security logs are reviewed daily to identify unauthorized access.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

USCG personnel and contractors accessing NPFC PRFLACS are required to have annual system security training which includes Privacy Act compliance training.



8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. NPFC PRFLACS is operating under an Authority to Operate, which was signed on 15 August 2006.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Users' profiles restrict system access. Practices are in place and used by system approvers to authorize specific user privileges and monitor actual access. Training on privacy and security is required annually from everyone with access to the system.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

Both. The Case Information Management System is a customized application of Oracle Financials' Project Accounting (PA) and Accounts Receivable (AR) modules. The Case Information Management System does not change data, functionality, or user privileges; it only upgrades the technology platform for the integrated application. The Claims Processing System and Certificate of Financial Responsibility System were built from the ground up.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity, security, and privacy requirements were defined and validated during systems analysis. Defined requirements and access controls were verified during system testing. All system enhancements are presented to the NPFC Configuration Control Board where security and privacy considerations are discussed prior to execution of the enhancement.

9.3 What design choices were made to enhance privacy?

User accounts, access restrictions, encrypted data transmission, Oracle security, and Windows Active Directory controls were used to ensure data integrity, privacy, and security.



Conclusion

NPFC PRFLACS is a system with sufficient controls to protect its data from inappropriate access. Account and access security complies with USCG guidelines and is enforced by the NPFC ISSO. Privacy data is limited to that required to perform NPFC's specified mission. Output from the system is protected by business practices that limit its dissemination outside of the NPFC.

Responsible Officials

Amy Becker, Acting NPFC Privacy Officer

George Cognet, NPFC Resources Management Division Chief

U.S. Coast Guard

Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security