National Oceanic and Atmospheric Administration (NOAA)

National Marine Fisheries Service (NMFS)
Office of Law Enforcement (OLE)
Law Enforcement Accessible Database System (LEADS)

Privacy Impact Assessment Statement

April 2009

Prepared by: William Stevens, NMFS OLE
Reviewed by: Sarah Brabson, NOAA Office of the Chief Information Officer

National Oceanic and Atmospheric Administration

Project: Law Enforcement Accessible Database System (LEADS)

Unique Project Identifier: 006-00-02-00-01-0511-00-404-139

IT Security System: NOAA4060

Project Description

The LEADS system was developed to replace the law enforcement portion of the Enforcement Management Information System (EMIS), with a modern, Web-based system to support Office of Law Enforcement (OLE) agent and officer needs by facilitating the entry, management, and reporting of OLE law enforcement data. It provides support to authorized agents, officers, and support personnel. Only they are authorized to enter information into the files, access that information, and respond to inquiries. EMIS will continue to support the case tracking functions for NOAA Fisheries General Council for Enforcement and Litigation (GCEL). The GCEL is responsible for prosecuting civil cases developed by OLE and for collecting fines imposed on those cases.

This PIA has been developed to comply with the requirement in Section 208 of the E-Government Act of 2002 (44 U.S.C. 36) and the Department of Commerce IT Privacy Policy.

1. What information is to be collected (e.g., nature and source)?

Both personally identifiable information (PII) and business identifiable information (BII) are collected. The personal and business information collected is pertinent to the stated law enforcement purposes for which the information is to be used. Only information that is required for establishing and implementing the LEADS law enforcement system is to be collected.

This does not constitute an information collection within the meaning of the Paperwork Reduction Act (PRA); therefore, approval by the Office of Management and Budget (OMB) is not required for this system. The information is collected by law enforcement personnel from the observation of vessels, review of documents, and information about owners and vessels that is available from other NOAA information collections that, if required, were approved by OMB.

The categories of information in LEADS are:

- *Names and Addresses* –Identifying information for individuals and businesses with which OLE has interacted; these names will be linked to other information such as vessels, violations, cases, and warnings.
- *Vessels* – File of all vessels with which OLE has interacted; includes permits and links to Name and Address and permits files; also includes vehicles related to warnings, violations, and other cases.

- *Cases* – Information relating to administrative, civil, and criminal violations that are the basis for OLE cases; the cases also include investigative support materials such as notes, photos, audio recordings and charts. This information provides the basis for the collection of fines and/or the prosecution of OLE cases.
- *Seized Property and Evidence* – Accounts for all seized property and evidence including perishable seized property and its immediate disposal; seized vessels, other non-perishable property and where it is stored; and chain-of-custody evidence tracking.
- *Arrests* –Records of all OLE arrests.
- *Management Information* –Daily, weekly and monthly summaries of OLE activities developed for authorized OLE managers and supervisors.
- *OLE Property* –Inventories of OLE property, including surplus property, issued to agents.
- *OLE Sworn Personnel* –Directory of OLE sworn personnel, including their training, assignments, and current work location.

2. Why is the information being collected (e.g., to determine eligibility)?

The information is collected for the purpose of ensuring compliance with federal and regional fishery regulations developed to manage fisheries and prevent over-fishing. The overall authority for federal fishery management is the Magnuson-Stevens Conservation and Management Act (16 U.S. Code 1801), as amended in 2006. Federal regulations may be found at 50 CFR 300 and 50 CFR 600-697.

The National Marine Fisheries Service (NMFS) Office of Law Enforcement (OLE) developed this system to help NMFS support the domestic and international conservation and management of living marine resources. OLE is responsible for enforcing compliance with 29 statutes pertaining to fishing, marine mammal protection, and endangered species protection. OLE enforces these statutes along the coastal waters of all of the United States, including Guam, American Samoa, and other US territories. Responsibilities range from floating fish processing factories in Alaska to pleasure boats in the Gulf of Mexico to fish dealers in New York City to the farmers in Oregon that border the spawning grounds of endangered salmon. As a law enforcement system, LEADS provides OLE law enforcement agents and officers with much quicker access to more complete data. The effectiveness and safety of OLE's agents and officers depends on this rapid access to complete information about vessels and the individuals on those vessels. This is especially important in potentially dangerous boarding situations at sea.

In the course of meeting its responsibilities, OLE collects and maintains information on individuals and businesses with which OLE has interacted. These include fishing boat owners who are expected to have licenses and permits to fish in US coastal waters; fish processing plant owners and dealers that purchase catches from these individuals; and other individuals that have been involved in cases in which there are violations of US laws.

3. What is the intended use of the information (e.g., to verify existing data)?

The information will be used to (1) detect instances in which the US fisheries laws as well as other US laws have been violated; and (2) develop case files that support fining and/or prosecuting these violators. The case files include information collected by the law enforcement officers or agents such as approved fishing licenses, type of fishing gear being used, and information on the catch. The case files also contain substantiating evidence such as sworn witness accounts, photographs, documents, and voice recordings. The case files support the collection of fines and/or the prosecution of these cases.

4. With whom the information will be shared (e.g., another agency for a specified programmatic purpose)?

LEADS personal information is shared only with authorized users who have a legitimate need to know. These records or information contained therein may specifically be disclosed as a routine use as stated below. The Department will, when so authorized, make the determination as to the relevancy of a record prior to its decision to disclose a document.

- In the event that LEADS indicates a violation or potential violation of law or contract, whether civil, criminal or regulatory in nature and whether arising by general statute or particular program statute or contract, or rule, regulation or order issued pursuant thereto, or the necessity to protect an interest of the Department, the relevant records in the system of records may be referred to the appropriate agency, whether federal, state, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute or contract, or rule, regulation or order issued pursuant thereto, or protecting the interest of the Department.

- A record from LEADS may be disclosed in the course of presenting evidence to a court, magistrate or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

- A record in LEADS may be disclosed to a member of Congress submitting a request involving an individual when the individual has requested assistance from the member with respect to the subject matter of the record.

- A record in LEADS may be disclosed to a contractor of the Department having need for the information in the performance of the contract, but not operating a system of records within the meaning of 5 U.S.C. 552a(m).

- A record in LEADS may be disclosed to authorized sworn agents or officers of other federal law enforcement agencies, such as US Coast Guard, or to a federally deputized agent or officer of a state law enforcement agency under a Joint Enforcement Agreement, for the purpose of detecting and prosecuting violators of federal fisheries laws and regulations.

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

Information in LEADS is collected by, and entered into the system by sworn OLE agents and officers or their support staff. Individuals and businesses are not asked to and do not provide any information for LEADS.

6. How will the information be secured (e.g., administrative and technological controls)?

Management Controls:

LEADS can only be accessed by authorized OLE personnel. The OLE does a thorough check on all of its personnel and contracting staff including local, state, and national checks of law enforcement databases, as appropriate for a law enforcement agency. LEADS can only be accessed via a secure NOAA network; both the network and the LEADS application require passwords that are issued only to those who require access to the system. Paper records related to LEADS are maintained in locked file cabinets at OLE facilities; these facilities require electronic OLE identification badges for entry.

Operational Controls:

Operational controls include securing all server and communications hardware and software associated with LEADS at NOAA Data Centers. The Data Centers are tightly controlled by card entry and staff to restrict access to the servers, their operating systems and databases. Plans are being implemented for contingency operations, including alternative processing sites at secure locations in accordance with Continuity of Operations planning for the U.S. Department of Commerce, NOAA's parent agency. Backups are performed on the processing databases every production day (Monday through Friday). The backups include all file directories (except the operating system directory) and databases. Additional operational controls include: (1) logical edit checks to ensure proper sequence of actions; (2) full auditing of all system transactions; (3) ability to "lock" sensitive files so that only specific authorized personnel have access, or even know about, the sensitive files; and (5) restricted access.

Technical Controls:

LEADS can be accessed through desktop computers at OLE facilities or via laptop computers carried by OLE field agents and officers. Desktop computers at OLE facilities are protected because, as mentioned above, entry into the facilities requires an authorized OLE badge. The laptop computers carried by field agents and officers will be password protected using *SecureDoc*® so that unauthorized users cannot gain access to laptop's files or to LEADS. Either from the desktop or laptop computer, to access LEADS the user must first access a secure NOAA national network. Network access requires a current password. Once on the network, the user must have an additional password to access the LEADS application. The LEADS System Administrator is responsible for issuing LEADS passwords.

LEADS is a browser-based system. This means that information is entered into screens presented to the users after they have logged on to LEADS. The information is not

retained in the user's computer once it is entered into LEADS. Agents or officers at remote locations, such as on board a vessel, can enter summary information into a special form on the laptop. The agent or officer transfers this information to LEADS at the earliest opportunity; it is not stored on the user's computer after that transfer. Because of the *SecureDoc*® protection explained above, this information is not accessible to unauthorized users of the laptop for the short time it may exist on the laptop.

Data Extract Logging and Verifying:

All logging and monitoring data is retained indefinitely as part of the record itself. Back up extracts are automatically taken form the LEADS database each night and they are retained on a secure server in the OLE data center for one night and are overwritten the second night automatically.

General policies for auditing Oracle production data and database usage include the following data extract logging and verifying controls:

- All data tables are constructed with four audit columns: a) created by; b) create date; c) last modified by; and d) last modified date. This feature ensures that a log entry is recorded whenever a new record is created or updated and by whom.
- History tables exist for active data tables. In addition to logging new record inserts and updates of existing records, the history tables record date and time of the change, the user making the change, and the nature of the change (i.e., old data and new data).
- Tables exist for monitoring successful and unsuccessful login to the system.
- Users log on using individual accounts with passwords (not shared accounts).

One identified risk is the inadvertent release of private information to unauthorized staff because the system is used in an open office setting. This risk is mitigated by the development and issuance to users of written policies and procedures regarding their responsibilities to safeguard the sensitive personal information in the in the system. User responsibilities are reinforced by training when an individual is initially granted access to the system and periodically thereafter.

This data is secured in compliance with the requirements of the Federal Information Security Act of 2002 (FISMA). A Security Certification and Accreditation (C&A) was completed for this system in June 2007. The C&A process is an audit of policies, procedures, controls, and contingency planning, required to be completed for all Federal Government IT systems every three years.

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a.?

No. The existing Privacy Act system of records notice (SORN) for NOAA-5, Fisheries Law Enforcement Case Files applies to the personal information in this system.

8. Are these records covered by an approved records control schedule?

Paper based Fisheries Violations Investigative Case Files are covered by Item 1513-01 in the NOAA Records Disposition Handbook., but a records schedule has not yet been

developed for the electronic records in LEADS. Under NMFS OLE policy, LEADS retains all records, including an audit of deleted records, indefinitely. A records retention schedule reflecting OLE policy will be developed by October 2009, in consultation with the NOAA Records Manager.

Program Contact Person:

KC Kleinman,
LEADS System Administrator
Kc.Kleinman@noaa.gov
(301) 427-2300 x105