National Oceanic and Atmospheric Administration (NOAA)

National Vessel Monitoring System
Privacy Impact Assessment Statement

April 2009

National Vessel Monitoring System

Privacy Impact Assessment Statement

Unique Project Identifier: 006-48-01-14-02-3168-00

IT Security System: NOAA 4060

Information Collections: OMB 0648-0202, -0372, -0404, -0441, -0445, -0478, -0519, -0544

Project Description:

The national Vessel Monitoring System (VMS) program provides near-real time fishing vessel monitoring, control and surveillance throughout the US Exclusive Economic Zone (EEZ), Pacific Ocean, and Atlantic Ocean.

For each monitored vessel, VMS provides, accurate to 100 meters, 365 days per year, 24 or more position reports per day (latitude and longitude). This continuous monitoring supports the achievement of compliance with regulations regarding open and closed seasons, closed areas, international boundaries and obligations. It also provides critical, life saving information to the Coast Guard in support of their response in Search and Rescue (SAR) cases.

The VMS stores each vessel's unique identifier and location in an Oracle database and displays the vessels on an electronic map using an off-the-shelf surveillance application, SmartTRAC. The information obtained through VMS is evidentiary in nature and used to prosecute violations of fishery regulations in administrative and civil proceedings.

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)?

The VMS database contains data such as:

- Vessel Name
- Permit numbers
- Permit types
- Coast Guard Documentation numbers
- State registration numbers
- Position information (current and archived)
- Unique Identifier of satellite transponder unit
- Contact e-mail address and/or phone number

Satellite transponders aboard each vessel transmit the position reports at given intervals, generally once an hour. Information received from the vessels is matched with the

vessel's registration data and the satellite transponder's unique identifier. This ensures that each position report is associated with the correct vessel. If there is any question to the accuracy of the data, the transponder unit can be removed from the vessel and tested for accuracy.

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.

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

The Vessel Monitoring System (VMS) helps ensure individual vessel compliance with regional and federal fishing regulations through transmitted position reports at given intervals. Vessel tracks can be analyzed to indicate trends or patterns of suspicious or unusual activity.

VMS is also used by the U.S. Coast Guard and other federal and international law enforcement agencies to enforce other federal laws and international treaties related to the prevention of over-fishing: the High Seas Fishing Compliance Act, the American Fisheries Act, the Atlantic Coastal Fisheries Cooperative Management Act, the Atlantic Tunas Convention Authorization Act, the Northern Pacific Halibut Act and the Antarctic Marine Living Resources Convention Act.

VMS data is also used by the U.S. Coast Guard in coordinating Search and Rescue (SAR) operations in addition to their law enforcement duties.

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

Internal - NOAA Office for Law Enforcement, the administrator of the Vessel Monitoring System program. All data within the user's region is displayed for the purpose of enforcing compliance with federal and regional fishery regulations. The Office for Law Enforcement (OLE) provides users with training on how to properly use the Vessel Monitoring System, as well as proper practices and procedures for handling sensitive information.

External - The U.S. Coast Guard Law Enforcement Information Data Base (LEIDB)/Pathfinder receives PII and other data in VMS through a continuous data feed. All information is displayed for the vessels in a given region. USGS uses this information is used for law enforcement as well as SAR operations. VMS data are secured by the U.S. Coast Guard in accordance with U.S. Coast Guard regulations regarding the use and disclosure of law enforcement sensitive data. U.S. Coast Guard personnel are trained in the use of VMS and the handling and disclosure of data in accordance with U.S. Coast Guard regulations. The LEIDB/Pathfinder PIA includes additional details regarding the protection PII in that system. VMS does not receive data from LEIDB/Pathfinder.

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 may individuals grant consent?

Individuals who decline participation with this program are not eligible for a commercial permit in the region or fishery that requires VMS. Participation in the VMS program is a condition for holding or obtaining a permit.

The information collected is used primarily for law enforcement purposes. There is no public disclosure or access to this data or the system. Individuals participating in this program have the option to enter multiple contact methods in the vendor registration form (secondary telephone number, secondary e-mail, etc.).

The name of the vessel owner can be retrieved from the applicable fishery permit database when required by the Office of Law Enforcement and/or the U.S. Coast Guard to investigate a possible violation. Retrieving such information is listed as a "routine use" in the Privacy Act Statement on all Sustainable Fisheries permit forms. The list of routine uses refers to instances in which information may need to be shared with another federal agency. The routine uses for fisheries permits are listed in the Privacy Act System of Records Notice (SORN) COMMERCE/NOAA-19 Permits and Registrations, which was published on April 17, 2008 in the *Federal Register* (73 FR 20914-18). The first routine use in NOAA-19 provides for the sharing of information with other federal agencies for law enforcement purposes.

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

Management Controls:

VMS contains law enforcement sensitive data. The loss of confidentiality could compromise ongoing criminal investigations. For this reason, encryption and closely managed user access were fully implemented in the system. There is no public access to VMS. All network communication is handled through a secure encrypted connection.

All user accounts are centrally managed through Microsoft Active Directory, and are individually assigned on the basis of least privilege (least privilege is the practice of granting the least amount of access possible to a user while still allowing fulfillment of job responsibilities). Accounts and access levels are created and managed also through the principle of individual accountability, and through periodic account audits.

Access is logged at the firewall level when the secure encrypted connection is initiated, as well as when a user logs into the system. Only users whose job requires access to the system can obtain a user account. The procedures for obtaining an account are documented in the System Security Plan.

Operational Controls:

The system is physically housed in an office building in Maryland, with a failover site located on the West Coast. The building is staffed by a contracted security firm five

days a week, and has existing physical security and fire protection controls including uniformed guard service during business and evening hours.

Physical access to VMS system hardware is restricted to authorized staff. The local area network (LAN) and server rooms are secured with access card doors. Access cards are provided only to VMS administrators and IT personnel.

In the event an outside technician is required, the technician is supervised and observed at all times by a member of the VMS IT Staff.

The system is housed in an area where appropriate environmental security controls are implemented. Environmental concerns include hurricanes, tornadoes, and lightning strikes. Precautions for these concerns are as follows:

a. The data is backed up at the end of each day and the backup tapes are stored offsite.
b. Computer servers and network equipment and software are off-the-shelf and readily available through multiple sites (including local sources).
d. The computer room is located in an inner office to allow protection from high winds, broken glass, and moisture.
e. Servers are all connected to uninterruptible power supplies
f. A fire extinguisher is located in the computer room.

Technical Controls:

Only system administrators have full access to the system. All other users have read-only access. Access is assigned based on the principle of least privilege.

All user accounts are centrally managed through Microsoft Active Directory.

Account and access level information are manually verified upon creation by the system administrator, based upon the user's roles and responsibilities.

System Administrators and IT staff are granted access according to their specific responsibilities. Each user within VMS has a unique account. The access level of each account is dependent upon the user's role within the system as well as his or her job responsibilities. The system owner and network administrator assign duties and responsibilities.

System privileges are assigned by the network administrator or system owner based on the individual's job requirements and the principle of least privilege. Privileges are limited to only those necessary for job requirements. Each user has an individual account assigned to him or her, providing accountability in the event of unauthorized system activity.

VMS 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 and is up-to-date. 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.

Data Extract Log and Verify:

1. All transactions on the database; including static data changes and data dictionary changes are recorded to archive logs. These logs allow a snapshot of the database to be reconstructed to any point in time and provide for identification of the exact SQL commands run by any user that modified the database structure or its data.

2. VMS users who run extracts through the provided application software have their permissions controlled within Citrix Metaframe to allow (or prevent) the saving of data to local storage or transfer via the clipboard – except in certain circumstances where the data is to be transferred for use in evidence and must be retained indefinitely on that basis. Temporary data that is not specifically stored by a user is automatically erased upon completion of each session.

3. Other authorized OLE, NMFS or NOAA users have access to VMS data through published SQL views. The data extracted by those applications would be retained subject to individual data retention policies of the destination system.

4. Users log on using individual accounts with passwords (not shared accounts). Multiple failed logon attempts will lock a user out and password complexity, reuse and locking policies are enforced.

These audit logs are reviewed by a system administrator approximately every 30 days, or upon notification of an event that merits inspection of the data. These logs are retained for 7 years.

The current Non-Disclosure Agreement (NDA) that must be signed by anyone accessing VMS is being revised to mandate the destruction/deletion of extracted data after 90 days unless there is a documented reason for retaining it longer (such as ongoing investigation, pending litigation, etc.) where it will be entered into LEADS as an exhibit in the case package related to that investigation. Only sworn personnel would have reason to retain data for 90 days or more.

The primary identified risk is inadvertent release of VMS data. This risk is mitigated by training of OLE staff when they are granted access to the system and periodically thereafter. Risks are also mitigated via system and application authentication procedures and auditing procedures.

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

No. Although it includes some personal information (e-mail addresses and phone numbers), the primary method of reference or data retrieval is by vessel name, not by personally identifiable information, and thus it is not a system of records as defined by the Privacy Act.

8. How long are these records retained? The response should include the retention period and the applicable records controls schedule. If there is not a records schedule, the response should so indicate.

A schedule for the disposition of these records has not yet been approved by the National Archives and Records Administration (NARA). A schedule is being developed and is expected to be approved by NARA no later than September 30, 2009. Pending approval of a records schedule, VMS records are not authorized for disposal and must be retained.

Contact: Eric Barton, VMS Plans and Programs
Ph: (301) 495-7110 or eric.barton@noaa.gov.