U. S. Department of Commerce
National Oceanic and Atmospheric Administration

National Marine Sanctuaries
General Support System
NOAA6602

PRIVACY IMPACT ASSESSMENT

June 2009

Prepared by: Darrah Bagley-Armstrong, National Marine Sanctuaries

Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer

National Marine Sanctuaries General Support System

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

IT Security System: NOAA6602

Project Description:

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy. The national program consists of thirteen sanctuaries and one marine national monument; each site has its unique objectives and diversities. The program manages and protects particularly designated areas of the nation's oceans and Great Lakes for their habitats; ecological value; threatened and endangered species; and historic, archaeological, recreational, and esthetic resources. The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Although each individual site has unique objectives, they all share the program's main purpose, i.e., to preserve, protect, and manage the nation's marine environment.

The ONMS creates major scientific and education programs and activities and implements daily management of 186,618 square miles of coastal and ocean waters. The ONMS uses information technology to provide a "hands-on" laboratory where people can see, touch, and learn about the greater ocean ecosystem. In other cases, the sanctuary is figuratively brought to the classroom and into public education awareness. The program communicates internally and externally through e-mail, brochures and flyers, program documents, Web sites, books, video, presentations, and newsletters. Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. In general, NOAA6602 provides network connectivity, Internet access, e-mail messaging, and software/hardware support.

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)?

All sites collect the following information: name, address, social security number (SSN), date of birth, telephone numbers, Dun and Bradstreet numbers for businesses, tax identification numbers for businesses. In addition, a few sites collect spouses' names and contact information, photographs, drivers' licenses, vessel registration information, demographical information, fishing licenses.

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

The information is collected for personnel actions, time and attendance entry, travel documents, emergency contact information, contract oversight, sanctuary permit oversight, damage assessment and restoration data, Office of Safety and Health Administration (OSHA) accident and injury reports, and as required by federal or state law or regulation.

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

Intended uses are: personnel, safety, security, emergency response, damage assessment, and restoration.

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

Internal sharing – site-to-headquarters, site and headquarters to NOAA.
External sharing – federal and state law enforcement agencies as required, state partner agencies, OSHA, other federal and state agencies as required.

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?

At each site, individuals may decline to provide information and/or to provide authorization either verbally or in writing to supervisor or volunteer coordinator for use.

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

Management Controls:

All sites grant, with supervisor approval, user access to data on an as-needed basis. IT Contacts and site management periodically review user access to determine whether continued access is required or whether access should be discontinued. Hard copies of data are stored in locked cabinets and kept according to records retention schedules and policies. System and software updates are performed as necessary and available. Systems are centrally scanned for vulnerabilities with most patches implemented directly at each site.

Operational Controls:

Each site maintains physical security for its equipment and hard copy data. Security measures differ at each site. Public access to equipment is restricted according to policies and procedures in place at each site. Data is backed up on varying schedules and backup media are secured. Privacy data access is restricted to users who need access as part of their official duties. All staff complete privacy training in accordance with NOAA content and schedule.

Technical Controls:

A Security Certification and Accreditation (C&A) in accordance with the requirements of the Federal Information Security Act of 2002 (FISMA) is current for this system. 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 Requirement:

Only two sites on NOAA6602 extract PII. One uses the data extracted and deletes it immediately. It is not stored. The other site restricts user access to the data and deletes electronic copies and shreds hard copies of the data within 90 days from end of use.

Most sites do collect hard copy PII data for data entry as part of their volunteer operations. This hard copy data, which is the agency's record copy, is stored in locked cabinets similar to copies of personnel records. Volunteer records are subject to retention as identified in Chapter 1600, Section 1609-14, of NOAA's Records Disposition Handbook.

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

No, a new system of records is not being created. The personal information in this system is covered by existing Privacy Act systems of records notices (SORNs), including:

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies
DEPT-20, Biographical Files
DEPT-19, Department Mailing Lists
DEPT-12, Investigative and Inspection Records
DEPT-13, Investigative and Security Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
OPM/GOVT-5, Recruiting, Examining and Placement Records
NOAA-11, NOAA Mailing Lists

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

Yes, both the paper input records and the electronic records are approved for disposition under Chapter 1600, Item 1609-14, of NOAA's Records Disposition Handbook.