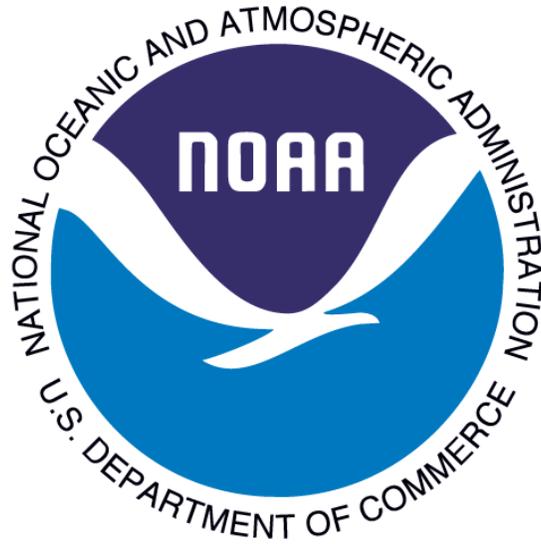


**U. S. Department of Commerce
National Oceanic and Atmospheric Administration**



**Office of National Marine Sanctuaries
General Support System
NOAA6602**

PRIVACY IMPACT ASSESSMENT

November 8, 2010

Prepared by: Jonathan M. Gordon, Office of National Marine Sanctuaries
Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer

Name-of-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.

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 patches implemented from a central configuration management system and 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. Staff members are required to complete privacy training in accordance with NOAA content and schedule.

Technical Controls (please address this specific request as part of your information here:

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](#).

NOAA6602 has developed an Audit & Accountability (AU) Policy and Procedure to provide guidance regarding the implementation of the following automated controls for logging and monitoring data extracts and reviewing logged information:

AU-2

For all server components of NOAA6602, audit results are written to logs anytime one of the following events occurs: hardware failure, system resource exhaustion, process error message, failed login attempt, operating system panic, remote file system mount failure, and any specific application message. Settings for audited events are reviewed as a part annual security plan updates.

AU-3

Each NOAA6602 system maintains its own set of logs and logs the following events: 1) security-related events such as login/logout and failed logins; 2) mail system events (who or what sent an e-mail and a destination address); 3) file transfers; 4) automated events; 5) hardware messages; and 6) system software package modification/update. Each log contains a date and time stamp along with the event being logged. Logging capabilities could be expanded to include other information if deemed necessary by the system administrator.

AU-11

NOAA6602 is under no standing specific legal requirement for log retention. Each subsystem configures its components to retain security logs to a maximum capacity or for a maximum length of time, or both (whichever comes first). Once the configured maximum is reached, logs are overwritten. This is deliberate; the availability of NOAA6602 systems is the priority and the existence of other security controls mitigate the risk of a major incident requiring an extended log history.

All audit logs are backed up to Linear Tape Open (LTO) tapes or portable disk-based hard solutions and stored offsite. To provide support for after-the-fact investigations, audit logs may be restored to either: (a) the original device on which the audit was made, or (b) a test system with which to examine the audit logs. The quarterly backup tapes are kept indefinitely.

In addition, logs are backed up on a daily basis via Backup Exec or Retrospect, and the tapes become part of the backup tape rotation. To provide support for after-the-fact investigations, audit logs may be restored to either: (a) the original device on which the event occurred, or (b) a test system with which to examine the audit logs.

A Security Certification and Accreditation (C&A) in accordance with the requirements of the [Federal Information Security Act of 2002](#) (FISMA) was completed for this system on July 23, 2010. 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.

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

7. 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:
8. DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
9. DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
10. DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies
11. DEPT-20, Biographical Files
12. DEPT-19, Department Mailing Lists
13. DEPT-12, Investigative and Inspection Records
14. DEPT-13, Investigative and Security Records
15. DEPT-14, Litigation, Claims, and Administrative Proceeding Records
16. OPM/GOVT-5, Recruiting, Examining

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](#). In addition, ONMS has implemented the following NIST 800-53 Media Protection controls to process both paper and electronic records:

MP-1

NOAA6602 adheres to procedures for information and media protection that were developed and implemented for NOAA6602, including managing backup tapes and storing them at both local and off-site storage locations.

All sensitive information is appropriately categorized and marked to indicate how it should be handled, processed, stored, and disposed. These procedures extend to

electronic media as well.

The NOAA6602 System Owner is responsible for ensuring media protection control policy and procedures are implemented. The NOAA6602 Information System Security Officer (ISSO) is tasked with drafting the policy and procedures for approval from the System Owner. The NOAA6602 ISSO is also responsible for the implementation of and updates to the procedures. The NOAA6602 ISSO may delegate portions of this responsibility, as necessary. This may include, but is not limited to, NOAA6602 subsystem leads and the NOAA6602 Configuration Control Team.

NOAA6602 uses DOC/NOAA IT policy and NIST Special Publications 800-53, Revision 1 (December 2006), at a minimum, in the development of formally documented procedures and best practices.

The procedures for this control family are routinely reviewed at least annually by appropriate system representatives (to include subsystem team leads or designates). If updates are needed, either new documentation may be generated reflecting the needed updates, or existing documentation may be updated with appropriate notations on the Errata page. The documentation will be stored in an appropriate folder on the system's SharePoint C&A repository. The System Owner (or designate) will review, comment, and approve the documentation before any actual changes are implemented. Documentation change history may additionally be kept through SharePoint versioning or via email. SharePoint documentation is routinely backed up and stored at both local and off-site storage locations. Access to these procedures and reports is based on a "need-to-know" basis. Rights and access to this information and any supporting documentation are granted by the System Owner (or designates).