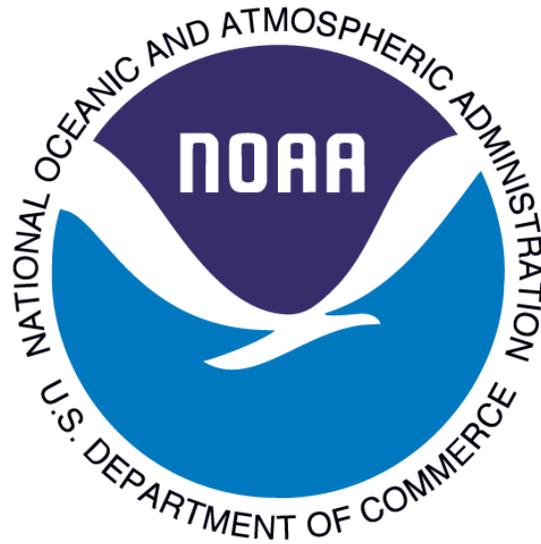


**U. S. Department of Commerce
National Oceanic and Atmospheric Administration**



**NOS Enterprise Information System
NOAA6001**

PRIVACY IMPACT ASSESSMENT

June 27, 2013

**Prepared by: Thomas K. Murphy, NOAA National Ocean Service, Office of the ACIO
Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer**

NOS Enterprise Information System (NOAA6001)

Unique Project Identifier: 006-00-02-00-01-0511-00 (Department of Commerce Consolidated IT Infrastructure)

Project Description:

The National Ocean Service (NOS) Enterprise Information System (EIS) is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services to NOS Headquarters and to NOS program and staff offices.

The NOS EIS provides Web application hosting services, which host and serve data-driven Web-based applications. Applications served from an internal Web server are accessible only to NOAA employees and contractors operating from within the NOAA network. These applications track information related to the internal operations of NOS. Applications served from public-facing Web servers may be intended for NOS and other subsets of NOAA, NOAA partners, or the general public.

NOS EIS Web applications collect, store and display data for these basic purposes:

- Administrative functions (replacing a manual process)
- Tracking of some action, information, request, task, or process related to the NOS/NOAA mission.
- Channel of information regarding NOS and NOAA to the general public.
- Response to a direct request initiated by a private individual.
- Point of contact information for participants in and sponsors of programs or events offered by NOS.

Several Web applications have been identified as requiring a Privacy Impact Assessment. These applications are the National Marine Sanctuary Permit Tracking application (*NMSPermit*), the Volunteer Net volunteer tracking application (*VolunteerNet*), the Constituents Database (*ConstituentsDB*) and the NGS Photo Ordering System (*NGS_Photos*). Of the four, NGS_Photos is the only public facing site; the other applications are for internal use only.

NMSPermit was developed internally for use by the headquarters and various field offices of the National Marine Sanctuaries program (*NMSP*) as part of the effort to track and manage the permit application process. It is used only by authorized NMSP personnel.

VolunteerNet was developed externally for use by the headquarters and various field offices of the National Marine Sanctuaries program (NMSP) to track and manage the assignments and hours of volunteers for different field sites. It is used only by authorized NMSP personnel.

ConstituentsDB was developed internally for the NOS Communications and Education Division for the purpose of tracking and contacting individuals who have either a stakeholder interest or a general interest in the mission, programs, and activities of the

NOS. Access may be extended to NOS program offices. Collected information is used to create mailing lists of NOS stakeholders and constituents.

NGS Photos was developed internally by the Special Projects Office for NOS's National Geodetic Survey program (NOAA6402). In an effort to automate the ordering of NGS/RSD photography data holdings, NGS/RSD has been working with SPO to develop a mechanism that will allow a user to mine our holding and make a request for ordering of specific aerial photography deliverables.

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

Personally identifiable information (PII) collected or stored by applications is limited to: name, address, phone, e-mail address, organization name, organization address, and position. In some limited-access applications, the PII is collected using some other method (mail, e-mail, fax, business card, etc.) and is entered by authorized NOS staff.

The information is collected from NOAA/NOS staff, NOAA/NOS partners, and members of the general public.

NMSPermit: The information is collected from private individuals and entered into the system by NOS staff. Actual collection is performed using some method outside the boundaries of the application (e-mail, mail, fax, etc).

VolunteerNet: The information is collected from private individuals and entered into the system by NOS staff. Actual collection is performed using some method outside the boundaries of the application (e-mail, mail, fax, etc). Information is shared only within the Sanctuaries program.

ConstituentsDB: The information is collected from private individuals and entered into the system by NOS staff. Actual collection is performed using some method outside the boundaries of the application (e-mail, mail, business cards, meetings & events, etc).

NGS Photos: Name, Company, Address, City, Email, State, Zipcode, Phone, and Fax are collected from private individuals who wish to order photos displayed online. The information is emailed from the application to NGS for processing of the order. The phone and fax fields are not mandatory for requesting an order.

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

In most cases the information is being collected to provide a method of contact (mailing lists, feedback, forwarding of requested information).

NMSPermit: Information is collected as part of the effort to track and manage the National Marine Sanctuaries permit application process. The information specifically considered to be identifiable is mainly used as contact information.

VolunteerNet: Volunteer Net tracks and manages the assignments and hours of volunteers for different National Marine Sanctuaries sites. The identifiable information allows hours to be tracked and also serves as contact information. The identifiable information is not used to make any kind of determination regarding the individual.

ConstituentsDB: Information is collected for the purpose of tracking and contacting individuals who have either a stakeholder interest or a general interest in the mission, programs, and activities of the NOS and NOAA. The identifiable information is mainly used as contact information for mailing lists. The identifiable information is not used to make any kind of determination regarding the individual.

NGS Photos: This information is being collected for the purpose of being able to complete an aerial photography order request in an automated fashion. The requestor will still have to call NOAA personnel for verification and order request completion.

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

NMSPermit information is used only by authorized NMSP personnel solely to track and manage the permit application process. The information specifically considered to be identifiable is mainly used as contact information and is not used to make any kind of determination regarding the individual.

VolunteerNet is used only by authorized NMSP personnel solely to track and manage the assignments and hours of volunteers for different field sites.

ConstituentsDB information is used to create mailing lists of NOS stakeholders and constituents.

In general, the legislation that created the various NOS programs includes provisions for the program to accomplish a mission. The mission may involve partnerships and educating the public. Collection and storage of information is part of accomplishing the legislated mission of those programs, the NOS, and NOAA.

NMSPermit: The National Marine Sanctuaries Act ([16 U.S.C. 1431 et seq.](#)) directs the Secretary of Commerce to designate and manage areas of the marine environment with nationally significant aesthetic, ecological, historical, or recreational values as national marine sanctuaries.

The National Marine Sanctuary Program (NMSP) has issued regulations to implement this act ([15 CFR Part 922](#)). These regulations exist to safeguard resources within sanctuary boundaries and include prohibitions on the conduct of some activities. Program regulations outline the procedure and criteria under which the NMSP will issue permits to allow certain activities beneficial to sanctuaries that would otherwise be prohibited.

NMFS [Guidelines for Submitting Applications for National Marine Sanctuary Permits and Authorizations](#) ([OMB Approval # 0648-0141](#)), Section IX – Reporting Burden states:

Submittal of the information requested in these guidelines is required to obtain a permit pursuant to NMSP regulations (15 CFR Part 922). This data is to evaluate the potential benefits of the activity, determine whether the proposed methods will achieve the proposed results, evaluate any possible detrimental environmental impacts, and determine if issuance of a permit is appropriate. It is through this evaluation that the NMSP is able to use permitting as one of the management tools to protect sanctuary resources and qualities.

VolunteerNet: Also as part of its mandate, the NMSP accepts volunteers who work with the Sanctuaries to fulfill the NMSP mission and the purpose of the Act.

ConstituentsDB: The collection of information for the purposes of educating and establishing relationships with NOAA's interested public is part of the NOS effort towards the NOAA-wide goal of supporting NOAA's mission (as identified in the NOAA Strategic Plan).

NGS Photos: This information will be used to complete a purchase order for the aerial photography requested through the system.

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

NMSP Permit: Only National Marine Sanctuaries Program staff members have access to this information. Field offices see only information applicable to that sanctuary for the purpose of tracking and retrieving permit application information and to maintain contact with permit applicants. The NOS Sanctuary office at Headquarters may see all of the information.

Externally, the NMSP has partnerships and joint management agreements with several state and federal agencies which establish the permit review process as reciprocal and shared.

According to the published [Guidelines for Submitting Applications for National Marine Sanctuary Permits and Authorizations \(OMB Approval # 0648-0141\)](#), completed applications are reviewed by NMSP program officials, on-site sanctuary personnel, and, when deemed necessary, peer-reviewed by outside experts. Also, certain non-identifiable permit information may be subject to FOIA requests. According to the Guidelines:

“Applicants are requested to indicate any information that is considered proprietary business information. Such information is typically exempt from disclosure to anyone requesting information pursuant to the Freedom of Information Act (FOIA). NOAA will make all possible attempts to protect such proprietary information, consistent with all applicable FOIA exemptions in [5 U.S.C. 552\(b\)](#). Typically exempt information includes trade secrets, commercial and financial information (5 U.S.C. 552(b)(4)). Personal information affecting an individual's privacy will also be kept confidential consistent with 5 U.S.C. 552(b)(6).”

For external peer review, personally identifiable information is excised.

Partners with which NMSP has a joint management agreement may request applications pursuant to that agreement, and vice versa, in order that both agencies might complete their review responsibilities. Permit application information is not shared with agencies that have no management responsibility over the activity in question.

Copies of the permit application are distributed by mail or e-mail.

VolunteerNet: Only National Marine Sanctuaries Program staff members have access to this information. Field offices see only information applicable to that sanctuary for the purpose of tracking hours and work by volunteers. The NOS Sanctuary office at

Headquarters may see all of the information. Information is not shared with external organizations.

ConstituentsDB: Information is shared with interested NOS administrative and program offices for purposes of creating targeted mailing lists for outreach and information. Information is not shared externally.

NGS Photos: This information will not be shared with anyone outside of NOAA. Only the individual within NOAA (specifically in the NOS National Geodetic Survey program) involved with the ordering process will have access to this information.

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?

NMSPermit: According to regulation the information is required as part of the permit application process. The application guidelines state that “Submittal of the information requested in these guidelines is required to obtain a permit pursuant to NMSP regulations ([15 CFR Part 922](#)).” The guidelines also state that:

“Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.”

The data are actually collected outside of the system and entered into the application by NOS staff. Applicants may submit amendments at any time as per the issued guidelines. If a permit is denied, applicants are informed of the appeal process. Corrected information will be entered by NOS staff.

VolunteerNet: The data are actually collected outside of the system and entered into the application by NOS staff. Sanctuary volunteers will become aware of errors through means beyond the boundaries of the EIS and will be given opportunity to make corrections to the information through a process also outside the boundaries of the EIS. Corrected information will be entered by NOS staff.

ConstituentsDB: The data are collected directly from individual via personal meetings, business cards, mail, e-mail, etc. Submission of business contact information is voluntary and use in mailing lists is understood as standard. Note that when information is used for mailing lists, individuals usually have a chance to respond with corrected information or a request to be removed as feedback from a mass mailing.

NGS Photos: The phone and fax fields are not mandatory for requesting an order, all other fields are mandatory. A disclaimer has been provided on the ordering page, explaining the use and purpose of this information.

On a more general level, any citizen may request information regarding data about him/herself that is stored in the NOS EIS by submitting a Freedom of Information Act

(FOIA) request. The process for doing this is on the Department of Commerce [FOIA Web page](#).

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

Management Controls

This is a moderate impact system.

A Security Assessment and Authorization (A&A) in accordance with the requirements of the Federal Information Security Management Act of 2002 (FISMA) was completed for the NOAA6001 system, on February 1, 2012. The A&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. NOAA6001 is under a continuous monitoring program and is assessed and re-authorized annually. NOAA6001 is currently (as of January 2013) being assessed and expects reauthorization in February 2013 (*reauthorized February 8, 2013*).

Operational Controls

Annual security awareness training with a section on data privacy is mandatory for all NOS employees and contractors. Training includes a section on Privacy Act information. Before deployment of an application, the NOS EIS requires that the application undergo a security scan and a code review. At those times, application access and roles are reviewed and tested.

Once a user has logged in, he or she has the ability to extract the information by printing or copying and pasting just by the functionality of the Web browser. At that point, use of the information is outside the boundaries of the EIS. This is mitigated by the annual security training and, to protect mobile information, all NOS laptops are fully encrypted.

In the cases where data are shared with federal or state partners, it is expected that those partners will have their own mandated requirements regarding the handling of privacy data.

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

The EIS application servers are protected from access outside of NOAA and outside of the NOS by a system of firewalls and routers. Whenever feasible, applications are hosted within the internally protected network to limit access to NOAA personnel only.

Technical access controls are in place on the Web and database servers and on the databases themselves to limit direct data access to authorized personnel (generally EIS administrators only, with exceptions authorized by both the EIS owner and application owner). Direct console access to EIS servers requires two-factor authentication and is limited to the system administrator with “least privilege” in place. (Least privilege is the

practice of granting the least amount of access possible to a user while still allowing fulfillment of job responsibilities.)

At the application level username/password combinations are required to further restrict the number of people able to retrieve the information. Role-based privileges are also in place for some applications to restrict the information viewed to a specific subset of that collected. Before production deployment of an application, the EIS policies require that the application undergo a security scan and a code review. At those times, application access and roles are reviewed and tested.

Privacy information is retrieved from the database by authorized staff members using either the same Web application with which the data was entered or by using an administrative extension to the base Web application. In either case, access is password protected, so only specifically authorized users may have access.

All applications which collect, store or process PII display the following banner on the login page. By logging in to retrieve data, users indicate that they understand and accept the following notice:

Information contained in this database will be used exclusively for the purposes of furthering the mission of the National Ocean Service (NOS) of the United States Department of Commerce (DoC) National Oceanic and Atmospheric Administration (NOAA).

- When not in use, personally identifiable information extracted from this database in digital format shall remain on NOAA systems and will be protected at all times.
- Hard copies of personally identifiable information extracted from this database will remain protected in the possession of NOAA personnel and will be used only for purposes identified by NOAA as part of its mission and operations.
- You agree to use this Web site and the information it contains in such a way as to abide by the privacy policies of the DoC and NOAA.

Application Specific

For ConstituentsDB, a privacy warning banner has been added to the login page alerting users that they are responsible for protecting the data once it leaves the EIS boundaries.

For NGS_Photos, this information will only be utilized on NOAA personnel computers that are completing the orders, as it has been conducted for several years. Once the order has been completed, the information will be deleted.

Data Extract Log and Verify:

Data extracts from these applications are not logged or monitored by the EIS. Neither the applications nor the EIS itself constitutes a major application. Applications and data are owned by the organizations for which the applications were developed, and data may be extracted for the purposes described above. It is up to the organizations to determine when the information is no longer needed and to destroy it at that point.

Note that in the case of NGS_Photos, data is not stored. It is sent directly to the data owner for processing.

Every year the IT system undergoes a thorough Continuous Monitoring for the Assessment and Authorization (A&A) process that is performed by the Line Office Security Team. The A&A process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) guidelines for continued operation. All security controls are reviewed and approved by the system and database administrators, developers, and managers prior to implementation.

A Security Assessment and Authorization was completed for the NOAA6001 system on February 1, 2012. NOAA6001 is under a continuous monitoring program and is assessed and re-authorized annually. NOAA6001 was reauthorized on 5-31-2013.

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-11, NOAA Mailing Lists](#) (being updated as of January 2013) applies to most of the personal information in this system. Other SORNs that apply include:

- DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
- DEPT-5, Freedom of Information and Privacy Request Records
- DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies
- DEPT-19, Department Mailing Lists
- DEPT-20, Biographical Files

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

The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. In accordance with [GRS 20, item 3](#), electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. In accordance with [GRS 20, item 3](#), the data is presently being retained indefinitely.

NMSPermits: The data for the Permit Tracking application remains in the database while the permit is active, and after that for as long as the Sanctuary office requires the permit record to be kept, in accordance with regulations governing the protection of Sanctuaries and the management of permit records. It is up to the Sanctuary office to make this determination. When a record is corrected, the corrected information overwrites the incorrect information, which is not retained.

VolunteerNet: Volunteer data is retained for as long as the volunteer is active, and after that for as long as the Sanctuary office requires the information for reporting and administrative purposes. It is technologically possible to delete a volunteer's record if the volunteer so requests it. It is up to the Sanctuary office to make this determination. When a record is corrected, the corrected information overwrites the incorrect information, which is not retained.

ConstituentsDB: Constituent data remains in the database until a) the data is determined to be incorrect and the constituent cannot be reached to make the corrections, b) the user no longer expresses an interest in being a constituent, or c) the user requests that it be deleted. Deleted records are purged on a daily basis. When a record is corrected, the corrected information overwrites the incorrect information, which is not retained.

NGS Photos: Data is not stored to a database. The information is sent via email directly to the NGS personnel responsible for fulfilling the order. When the email arrives in the inbox of the designated NGS personnel, the message will be deleted from the mail server. After that, the order will be in the possession of designated NGS staff and it will be handled in accordance to procedures that should already have been defined by the NOAA6402 information security system for handling orders prior to the web application being built.

Document updated: January 29, 2013