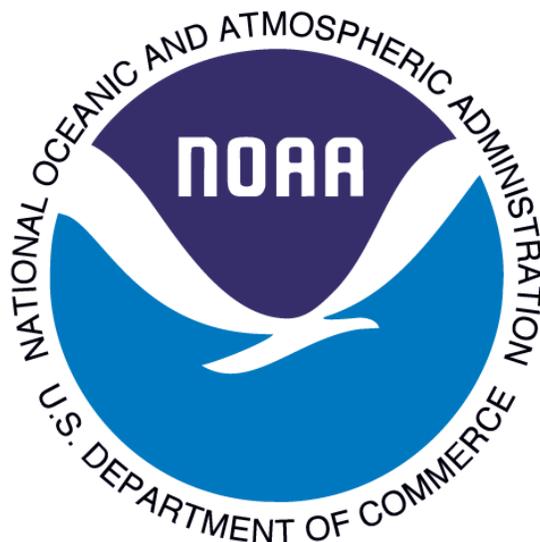


**U. S. Department of Commerce  
National Oceanic and Atmospheric Administration  
National Ocean Service (NOS)  
Management and Budget Office**



**Web Application Subsystem (WAS)  
Privacy Impact Assessment Statement**

**January 2010**

Prepared by: Cheryl L. Marlin, Information System Security Officer  
Reviewed by: Sarah Brabson, NOAA Office of the Chief Information Officer

# Web Application Subsystem (WAS) Privacy Impact Assessment Statement

**IT System:** Web Application Subsystem (WAS)

**ID Number:** 006-00-02-00-01-0511-00 (Department of Commerce Consolidated IT Infrastructure)

**OMB Approval Number:** 0648-0141

## **System Description:**

The National Ocean Service (NOS) Enterprise Information System 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.

One of the component subsystems is the Web Application Subsystem (WAS), which hosts and serves 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.

The Web applications in the WAS primarily 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.

The Web applications hosted by the WAS that require a Privacy Impact Assessment include the following: EstuaryLive ([ELive](#)) public facing registration application; National Marine Sanctuary Permit Tracking application ([NMSPermit](#)); Volunteer Net volunteer tracking application ([VolunteerNet](#)); Constituents Database ([ConstituentsDB](#)); NGS Photo Ordering System ([NGS\\_Photos](#)); and IOOS Web Request System ([NOAA IOOS](#)).

[ELive](#) registration was developed internally for the National Estuarine Research Reserve System ([NERRS](#)). *ELive* is an online estuarine education program. Teachers register and, on the day of the program, they go online with their classes to participate. The information is used to send material and request feedback.

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.

NOAA IOOS was developed by an IOOS contractor as a database to maintain user requests for enhancements to the NOAA IOOS Web site.

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

Personally identifiable information (PII) collected or stored by applications in the WAS 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.

ELive: Information is entered directly by the private individual.

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, e-mail, state, zip code, phone, and fax are collected from private individuals who wish to order photos displayed online. The

information is e-mailed from the application to NGS for processing of the order. The phone and fax fields are not mandatory for requesting an order.

NOAA IOOS: Name, telephone number and e-mail are collected from NOAA employees and partners, both governmental and non-governmental. Phone numbers and e-mails are being collected so IOOS Web administrators can collaborate with the partners regarding their requests for changes to the official IOOS Web site.

## **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).

ELive: Teachers complete a registration form to participate in the EstuaryLive online program. The identifiable information is mainly used as contact information to send material and request feedback. Neither the identifiable information nor the analyses are used to make any kind of determination regarding the individual.

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.

NOAA IOOS: Phone numbers and e-mails are being collected so IOOS Web administrators can collaborate with the partners regarding their requests for changes to the official IOOS Web site.

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

ELive registration information is used to send material and request feedback. Statistical analysis is performed on a year's registrations at the end of that year.

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.

ELive: Under the Coastal Zone Management Act ([CZMA](#)), National Estuarine Research Reserves are federally designated "to enhance public awareness and understanding of estuarine areas, and provide suitable opportunities for public education and interpretation." The information is collected as part of the registration process for an educational program and is needed to send materials that support and enhance the educational experience.

National Estuaries Day and its feature event, EstuaryLive are sponsored by NOAA's National Estuarine Research Reserves in collaboration with the Environmental Protection Administration (EPA) National Estuary Program (NEP). The [NEP](#) was established by Congress in 1987 to improve the quality of estuaries of national importance. The Reserves and NEP have a unique partnership and they work together to protect estuaries around the country. That partnership does not have an official Memorandum of Understanding or Memorandum of Agreement in place; the development of such an agreement is beyond the scope of the WAS.

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.

NOAA IOOS: Each of 17 federal agencies involved in the Integrated Ocean Observing System is a member of the Interagency Working Group on Ocean Observations (IWGOO), which was established by the Joint Subcommittee on Ocean Science and Technology and charged with advising and assisting the JSOST on matters related to ocean observations. The IWGOO recently voted to allow NOAA to change the Web site – [ioos.noaa.gov](http://ioos.noaa.gov) – from a Web site that solely represents NOAA's interests in IOOS and instead turn the site into the main Web site representing all parties involved in IOOS. As such, we need a better format to track and manage the many Website change requests expected from IOOS partners. Our answer to this is this new, dynamic, Web request system.

The collected PII will not be checked for accuracy. It collected only for contact purposes. The Web site requests will be reviewed by NOAA IOOS employees for content. We will only act on appropriate change requests. If there is a question as to the nature of the request, the request will be reviewed by NOAA IOOS management to make the call as to its appropriateness or accuracy.

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

ELive: Internally, contact information is used within the Estuaries program to maintain contact with ELive registrants. Geographical information is used for statistical analysis.

Because the EstuaryLive event is co-sponsored with the U.S. EPA's National Estuary Program, registration information (including identifiable information) collected by the application and statistical data are shared with that agency. The personally identifiable information is used to maintain contact with program registrants.

NMSPermit: 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.

NOAA IOOS: IOOS is the only organization that is using this information. There is no sharing.

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

ELive: Identifiable information is required in order to receive material related to the ELive! event. Explanation and links to the NOAA privacy policy are provided. No additional options are needed or given. Registrants may contact the administrators through the Web site to have their names removed from the registrant list.

NMSP Permit: 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 WAS and will be given opportunity to make corrections to the information through a process also outside the boundaries of the WAS. 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.

*NOAA IOOS:* The information will be entered by an administrator now and not the user. The user will have requested access to the system and will be aware that the information is being entered. The fields collected are username, e-mail and password. Users may, but are not required, to provide phone numbers. Since the information is only used internally as a means to communicate with the user and is not shared, there are no additional uses that require user consent.

On a more general level, any citizen may request information regarding data about him/herself that is stored in the WAS 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 technical controls)?**

### *Management Controls*

A Security Certification and Accreditation (C&A), in accordance with the requirements of the [Federal Information Security Management Act of 2002](#) (FISMA), was completed for the NOAA6001 system, of which the WAS is a subsystem, on January 30, 2009. 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

### *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 WAS 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 WAS. 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*

The physical WAS is 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 WAS administrators only, with exceptions authorized by both the WAS owner and application owner). Direct console access to WAS 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 deployment of an application, the WAS Subsystem requires 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. In the case of *ELive*, where data is shared with the U.S. Environmental Protection Agency, appropriate staff within that agency’s programmatic office have been given a username and password combination which allows them to access the application via the Web and view the collected data

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 WAS boundaries.

For ELive, data is shared with a partner. The partner is another federal government agency which has and is expected to implement its own requirements, training and awareness, and controls regarding PII and retention of data.

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.

For NOAA IOOS, users must log in to use the system. Access to data is based on roles. Non-IOOS users may only view their own information. Data is being retained as contact information as long as the user remains an active user of the system.

*Data Log and Verify Requirement*

Office of Management and Budget (OMB) Memorandum [M-06-17](#), Safeguarding Against and Responding to the Breach of Personally Identifiable Information, requires that agencies log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required. The information collected by the WAS applications is not sufficiently sensitive, within the meaning of M-06-17 (note 7), to warrant the implementation of a log and verify system. The management, operational, and technical controls described above are adequate to ensure the protection of the non-sensitive information that is collected or maintained in these applications.

**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](#) 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 disposition 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.

*ELive*: EstuaryLive registration data is archived once a year, usually in October. The data is exported to a Microsoft Excel spreadsheet and given to the NOAA/NOS/NERRS division education coordinator. Before data is archived, an individual's data may be deleted at the individual's request. 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 e-mail directly to the NGS personnel responsible for fulfilling the order. When the e-mail 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.

*NOAA IOOS*: Data is being retained as contact information as long as the user remains an active user of the system.

**System Contact:**

Cheryl L. Marlin

Information System Security Officer

(301) 713-1156 x218

[cheryl.marlin@noaa.gov](mailto:cheryl.marlin@noaa.gov)