U. S. Department of Commerce
National Oceanic and Atmospheric Administration
National Ocean Service (NOS)
Coastal Services Center

Coastal Services Center Information Technology Support System NOAA 6101

Privacy Impact Assessment Statement

May 2011

Prepared by: Chuck Baxley, Information System Security Officer

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

Record of Changes/Revisions

This NOAA6101 Privacy Impact Assessment (PIA) is a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to this document are recorded in the Change/Revision Record below. This record shall be maintained throughout the life of the document.

Change / Revision Record				
Ver. No.	***Date***	***Description of Change***	***Pages Affected/ Section***	***Change Made By***
1.0	2008-4-3	Initial document	All	Mike Warren
2.0	2010-9-1	Update format and PII requirements	All	Mike Warren
2.1	2011-1-14	Updated identification of websites and databases containing PII	All	Jason Marshall
2.2	2011-2-22	Integrated software products and services with PII requirements	All	Jason Marshall
2.3	2011-3-14	Incorporate comments from Sarah Brabson	All	Mike Warren
2.4	2011-10-27	Updated identification of websites and databases containing PII	Section 2	Jim Boyd

Acronyms Used in the Privacy Impact Assessment			
BII	Business Identifiable Information	MARS	Management Analysis Reporting System
CBS	Commerce Business System	NARA	National Archives and Records Administration
COOP	Continuity of Operations Plan	NOAA	National Oceanic & Atmospheric Administration
CSC	NOAA Coastal Services Center	NOS	National Ocean Service
DOC	U.S. Department of Commerce	OPM	U.S. Office of Personnel Management
GRS	General Records Schedules	PII	Personally Identifiable Information
		WAS	Web Application Subsystem
		WebTA	NOAA's Web Time & Attendance System

Coastal Service Center IT Support System

Privacy Impact Assessment Statement

Unique Project Identifier: NOAA6101

System Description:

System NOAA6101 is a general support system used to ensure the Center's scientific and internal administrative / operational needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services to the National Oceanic and Atmospheric Administration's (NOAA) Coastal Services Center (CSC) located in Charleston, SC, CSC field offices, and remote staff. The system enables CSC to achieve its mission, which is to support the environmental, social, and economic well being of the coast by linking people, information, and technology. The Center assists the nation's coastal resource management community by providing access to information, technology, and training, and by producing new tools and approaches that often can be applied nationwide.

Two of the component subsystems are the file servers and Web Application Subsystem (WAS). While the file servers store and serve up administrative and operational data, the WAS 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 internal applications track information related to the Center's operations / administration. Applications served from public-facing Web servers may be intended for CSC and other subsets of CSC, NOAA, other federal agencies, customers, partners, and/or the general public.

The file servers and Web applications in the WAS primarily collect, store, and display data for these basic purposes:

- Administrative functions (replacing a manual process),
- Employee/Contractor/Intern information needed for personnel, security, performance evaluation, merit rewards, training, travel, etc.,
- Review of applicant information (e.g., information submitted in response to requests for proposals and/or in response to a solicitation),
- To track information, requests, tasks, actions, or processes related to the CSC / NOAA mission,
- As a channel of information regarding CSC, National Ocean Service (NOS), and NOAA to the general public.
- In response to a direct request initiated by a private individual,
- Collecting contact information for participants in (e.g., trainees) and sponsors of / partners in programs / events offered by CSC.

The Web applications hosted by the WAS and internal file server datasets that require a Privacy Impact Assessment include the following public facing websites : www.csc.noaa.gov and collaborate.csc.noaa.gov.

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

   Personally identifiable information (PII) collected by NOAA6101 includes name, address, phone, e-mail address, organization name, organization address, and position.

   This personally identifiable information is collected from NOAA/NOS staff, NOAA/NOS partners, customers (e.g., trainees), and members of the general public.

   Passport numbers are collected for foreign nationals who visit NOAA6101.

   Personally identifiable information is collected both manually by staff using required forms, mail, e-mail, fax, and business cards. Information is entered by authorized CSC staff into the proper storage facility (e.g., data base, secure paper files, etc.).

   CSC also uses web based applications to collect information from the public who choose to participate in the web based services and information provided by CSC.

   In addition, NOAA6101 stores scientific and geospatial data required to support mission accomplishment, which are not PII or business identifiable information (BII).

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

NOAA's Coastal Services Center's Management and Budget Division collects data containing personally identifiable and business identifiable information (BII) for internal government operations / administrative processes. The processes include:

- Employee / Contractor / Intern information needed for personnel, performance evaluation, merit rewards, training, travel, accident reporting, etc.
- Employee / Contractor / Intern / Visitors / Foreign National information required by DOC and/or OPM for security purposes and/or background checks. Passport numbers are collected for foreign visitors.
- Employee (including federal and contract staff) emergency contact information for use in call trees, Continuity of Operations Plan (COOP), etc. which includes names, phone numbers, and addresses.
- Employee (includes federal staff and contract staff) vehicle information for use in parking passes / facility access.
- Employee (including federal staff and contract staff) photos for internal staff locator directory.
- Applicant information submitted in response to requests for proposals and/or in response to a solicitation,
- Mailing lists, and
- Business contacts.

Other PII being collected by Internet public services Web applications includes:

- CRIS: Center Resource Information System contains current information on staff, including phone numbers, names, email addresses, emergency contacts and relatives. The system is used to maintain up to date records on staff contact information.
- TOMIS: Task Order Management Information System
- DAV: Data Access Viewer receives requests for data from the public. Emails are stored to provide a method of contacting the requester when the data is ready for pickup on the Center FTP site.
- CSC Contact Management System: Centralized contact management system used to host data from customers who have requested data, participated in conferences, meetings and trainings offered by the Center.
- Hazards Toolkit: contains contact name and email addresses of staff within the CSC Hazards program.
- Pacific Islands: Resilience: contains a list of projects and their associated Point of Contact with email and phone number.
- Coastal Storms Program: contains a contact database that lists contract offices, the Point of Contact name, email and phone numbers.

- CSC Clearinghouse: contains a repository of customers who have requested products from the Center from the web site. This system captures names, addresses, email addresses and phone numbers of customers requesting information.
- Training Tracking System: collects information on training courses, hosts and participants to Center coordinated training programs.
- Foreign Visitor Requests: manually collects information from the foreign visitors coming to the Center. All information is required per DOC PII Policy and Foreign National Processing[1] guidance as well as the FLETC Foreign National Visitor Process[2].
- Coastal Training Network Site – Contains a repository of partner/collaborator/stakeholder information related to training programs and activities. This system captures (in a standardized manner) names, addresses, email addresses, phone numbers, and organization
- Gulf of Mexico Climate Inventory Site - Contains a repository of partner/collaborator/stakeholder information related to climate projects and activities in the Gulf of Mexico. This system captures (in a standardized manner) names, addresses, email addresses, phone numbers, and organization.
- GeoTools Conference Site - Contains a repository of partner/collaborator/stakeholder information related to conference attendance and interest. This system captures (in a standardized manner) names, addresses, email addresses, phone numbers, and organization.

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

The system NOAA6101 has two purposes. The first purpose is to develop and support CSC efforts to meeting its scientific mission, which is to build capacity for informed decision making about our coasts by providing access to information, technology, and training, and producing new tools and approaches that often can be applied nationwide. The nation’s coastal resource managers are the Center’s primary customers, but the Center also assists other Federal agencies and non-federal partners. The second purpose is to provide internal operational / administrative support including office automation applications, file services, and print services. Specifically, personally identifiable information and business identifiable information are used for:

- PII and BII submitted to NOAA’s Coastal Services Center’s Management and Budget Division are used for the purposes for which it was gathered (e.g., Request for Proposals, background checks, emergency contact information, etc.) as stated in question 1.
- PII and BII submitted through public web sites are intended to support the accomplishing the CSC’s primary scientific mission (collecting information on constituents and users of CSC products and services) as articulated in the paragraph above.

[1] http://deemedexports.noaa.gov/Documents/Message_on_Electronic_Transmission_of_PII.pdf

[2] https://shipslog2.csc.noaa.gov/content/csc_info/Divisions/M&B/III._Program_Areas/a._Acquisition_and_Facility_Services/II._Facility_Services/3._Security_and_Visitor_Notifications/Guidance_-_Foreign_Visitor_Flow_Chart_with_Days.pdf

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

PII and BII submitted to NOAA's Coastal Services Center's Management and Budget Division are used for the purposes for which it was gathered and are only shared with appropriate staff. Appropriate staff refers to either federal or contract staff who have a need to know the data for completion of their job duties (e.g., timekeepers, procurement officers, supervisors, etc.). The examples that follow are not all inclusive. Rather, these examples are intended to provide data on how PII and BII is managed in specific instances.

- *Foreign National Visitors:* Only the information needed to complete security requirements is gathered. Information includes passport numbers, visa numbers, etc.. Information is shared with Department of Commerce Eastern Regional Security Office as well as with staff required to complete forms necessary for security check. This information is kept in secure location (e.g., locked cabinet in access controlled facility) until security approvals are granted and the foreign national visit has been completed. Then, this information is destroyed.

- *Emergency Contact Information:* This information is stored in our Center Resource Information System (CRIS) and is shared only with appropriate staff for call tree use. Call trees are provided to the employee's appropriate Division Chief and /or Program Manager for use when the call tree is activated. The Facilities manager of the NOAA Coastal Services Center may also access / use this information for emergency purposes. This information is not available to other federal or contract staff.

Other PII collected are shared as follows:

- PII and BII information collected through the CSC website will be stored internally in a secured relational database and used exclusively for ensuring completion of the product or service for which the information is being captured as listed under Question 2 (above).

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.

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?**

   PII and/or BII submitted to NOAA's Coastal Services Center's Management and Budget Division are used only for the purposes for which they were gathered. Should a potential contractor / vendor, other type of applicant (e.g., grant), or invitational traveler not wish to provide certain data (PII and/or BII), these individuals / companies may decline to do business with us.

   PII data collection process does not *typically* involve the collection of new information from individuals, but uses information previously provided as part of the individual's entry to duty processing, application for a security clearance, etc. However, employees (including both federal and contract staff) are required to keep their emergency contact and vehicle information current by updating / reviewing it at least once per year. Corrections may be made anytime the staff member feels it is necessary. The emergency contact information provided is not checked against other sources by CSC. There is no opportunity to decline to provide this information once employment as a federal or contract staffer has been accepted.

   Other PII collected may be declined as follows:

   All public facing web sites (listed under Question 2 above) provide explanation and links to the NOAA privacy policy. No additional options are needed or given. Users of these products may contact the administrators through the Web site to have their names removed from the registrant list.

   The data are actually collected outside of the system and entered into the CSC subsystems by CSC staff. Users may submit amendments at any time as per the issued guidelines.

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

Administrative Controls:

PII and BII submitted to NOAA’s Coastal Services Center’s Management and Budget Division are used for the purposes for which they were gathered. In accordance with internal operational / administrative processes, some PII and BII are kept in secure paper filing systems within the facility.   ccess to these secure file rooms / cabinets is restricted to federal or contract staff who require access to this information to complete their assigned duties.   These files are managed in accordance with the General Records Schedules that cover records common to several or all agencies of the Federal Government. The General Records Schedule includes several types of records kept by the Management and Budget Division pertaining to civilian personnel, fiscal accounting, procurement, communications, printing, and other common functions.

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 NOAA6101 system, of which the WAS is a subsystem, on May 18, 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.

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.

The workstations and computer rooms are located at federal facilities and have physically controlled and monitored access. All systems are on a secure private network protected by network firewalls as detailed in the CSC IT Security Plan.

Data is backed up by the IT staff as part of the COOP procedure and rotated off site.   The file servers are fully backed up monthly with incremental backups done daily. Data is restricted to the least number of users that requires access to the information. The applications are not accessible to the public, and any user must be authorized to have access to the application.

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. t 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 and communications channels are secured using HTTPS, so only specifically authorized users may have access. In the case where data is shared with partners, 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 link to the NOAA Privacy Policy on the page. By logging in to retrieve data, users indicate that they understand and accept the guidelines within the NOAA Privacy Policy.

For file servers, access controls are implemented on all systems through the use of system usernames and passwords as well as database (application) usernames and passwords. NOAA 800-53R1 access controls are enforced for access to CSC systems and applications. System access is logged centrally collected using EventSentry and manually and reviewed daily for any anomalies. Password length and duration of validity follow Department of Commerce standards as outlined in the IT Security Program Policy and Minimum Implementation Standards.

Specifically, access is limited only to staff needing access using Windows using groups which have been assigned roles and applied to access control list which conforms to the C&A technical control AC-3 which enforces assigned authorizations for controlling access to the system in accordance with applicable policy and control AC-3(1) which requires the information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. AU controls are used to audit log on and log off attempts. They are not used to record successful or failed reads and writes because it would overwhelm the system and the ability to sift through the logs collected through EventSentry.

If staff has a role to access files containing PII data, they are added to the appropriate group.

A complete list of access controls is in the NOAA 6101 C&A document NOAA6101 Initial Control Verification Report.xls.

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 May 18,

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.

A security assessment for this process has been completed in order to ensure adherence to guidance outlined in the FIPS-201 and its supporting publications as a part of the C&A process.

PII data on file servers is not gathered by database extract. The files are created using the technical controls identified in the IT Security Plan (described above) and the Security Certification and Accreditation (C&A) process. The files have an operational need to exist greater than 90 days.

Application Specific:

For *all websites*, a privacy policy link is included in the standard NOAA web site footer alerting users that they are responsible for protecting the data once it leaves the Center boundaries.

For *TOMIS*, 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 DAV, 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 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?

No. System NOAA6101 is not a Major Information System. Internal data stored on the system is done as an efficient electronic collector for information being input to other official systems or printed to be placed in an official paper file systems. Backups of data are made only for disaster recovery. Backups are not provided for archival purposes as outlined in the system COOP because the system is not an official source of records.

Original data for archival purposes are kept in 1) official paper filing systems (see also #6 Administrative Controls) where required or needed, and 2) off site IT systems such as Commerce Business System (CBS), Management Analysis Reporting System (MARS), Travel Manager, NOAA WebTA, Grants Online, NOAA Web-based Accident/Illness Reporting System, and Sunflower (NOAA Property Management System). These official records and associated retention periods are covered under 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.

All websites: The data request remains in the database while the request is active, and after that for as long as the products' system administrators require the record to be kept, in accordance with regulations governing the protection of records. It is up to the program management team who owns the site to make this determination. When a record is corrected, the corrected information overwrites the incorrect information, which is not retained.

System Contact:
Chuck Baxley
Information System Security Officer
(843) 740-1218
Chuck.Baxley@noaa.gov

Approved by Jonathan Cantor, Department of Commerce Chief Privacy Officer, May 12. 2011.