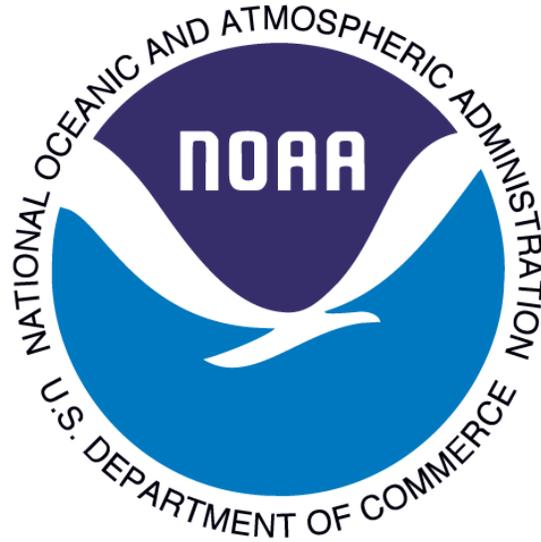


**U. S. Department of Commerce
National Oceanic and Atmospheric Administration**



***National Centers for Coastal Ocean Science (NCCOS)
Research Support System
NOAA6301***

PRIVACY IMPACT ASSESSMENT

January 17, 2013

Prepared by: Linda Matthews, NCCOS Information System Security Officer

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

National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

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

Project Description:

NOAA6301 is a General Support System for the National Centers for Coastal Ocean Science (NCCOS) Program Office of the National Ocean Service (NOS) Line Office. NCCOS is comprised of five Centers and associated research facilities located in Silver Spring, MD; Charleston, SC; Beaufort, NC; Seldovia, AK and Oxford, MD. Each Center has a specific mission contributing to the overall mission of the Program Office along with unique partnerships and cooperatives established to support and further strategic science goals.

This System is an integrated collection of subsystems designed to provide the necessary shared services for the geographically dispersed operational components. Subsystems are Local Area Networks (LANs) resident in Silver Spring, Maryland; Beaufort, North Carolina; Charleston, South Carolina; and Oxford, Maryland. They are either physically and/or logically connected through WAN links. Subsystems are as follows:

- National Centers for Coastal Ocean Science (NCCOS) SSMC (Silver Spring Metro Center) Local Area Network (LAN), Silver Spring, MD;
- Center for Coastal Fisheries and Habitat Research (CCFHR) Local Area Network (LAN), Beaufort, NC;
- Center for Human Health Risk (CHHR) at Hollings Marine Laboratory (HML) Local Area Network (LAN), Charleston, SC;
- Center for Coastal Environmental Health and Bio-molecular Research (CCEHBR) Local Area Network (LAN), Charleston, SC; and,
- Center for Coastal Environmental Health and Bio-molecular Research at Oxford (CCEHBRO) Local Area Network (LAN), Oxford, MD.

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

This General Support System (GSS) collects and stores information that consists of basic identifying information about employees, contractors, volunteers, and partner agency staff who are facility occupants or system users or federal grant requestors. The information is maintained as a supplement to other records for purposes of managing job vacancies, developing statistical reports lending to budget execution and human resource activities, Continuity of Operations (COOP) execution, and performing other related administrative tasks, e.g., training, travel, awards, facility management, and NOAA training requirements in support of the Diving and Small Boat program.

Information temporarily stored to manage job vacancies may include: full name, home address, home phone number, e-mail address, educational background, and employment

history. Information maintained for COOP and other administrative processes includes: full name, grade level and/or position within the organization, role/responsibility, home address, home phone number, and cell phone number when applicable.

In addition, information in identifiable form may be collected to facilitate public education, outreach or collaboration with partners on research projects, or grant review activities.

For this second group of activities, we may temporarily store the name, address, e-mail address, telephone number, organizational information, employment history, business or organization employer identification number (EIN) and educational history of private individuals, businesses or organizations. Social Security Numbers are not requested. These individuals, businesses or organizations may be workshop participants, grant applicants, business contacts, members of mailing lists, etc. They may also be job applicants. In all cases the information is voluntarily submitted.

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

The information is collected for the purpose of facilitating completion of required business processes. Processes include managing job vacancies, developing statistical reports leading to budget execution and human resource activities, the grant review process, COOP execution and performing other related administrative tasks, e.g., training, travel, awards, facility management, security clearance requests, NOAA Common Access Card (CAC) issuance, NOAA training requirements in support of the Diving and Small Boat program. In addition, information in identifiable form may be collected to facilitate public education, outreach or collaboration with partners on research projects, or grant review activities.

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

The information is intended to be used to complete required business processes described above. There are no other uses of the data.

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

Collected information that is destined for a NOAA or DOC managed business process is provided to other government or state agencies through NOAA and DOC systems. No other collected information is shared with other than NOAA6301 system authorized personnel. Access to information collected and maintained within the system boundary is determined by the requestor's role in the organization and is controlled within the boundary of the NOAA6301 Research Support System as detailed in Question 6 below.

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?

Employees and contractors are required to provide their personally identifiable

information (PII) as a condition of employment. Although providing information is voluntary in every situation, individuals, businesses and organizations are made aware that omissions may impact their employment, funding opportunities, or opportunity to participate in activities. No Social Security Numbers (SSN) are collected. The information collected is relevant to the task(s) only.

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

Management Con Management Controls

National Institute of Standards and Technology Special Publication 800-53 (NIST-800-SP 53), Recommended Security Controls for Federal Information Systems and Organizations, rev. 3, August 2009, identifies security controls for high, low, and moderate impact systems. The Research Support System is categorized as moderate impact, and its security controls are continuously monitored every year to ensure compliance with operational, management, and technical controls established by the Department of Commerce. The current Authorization to Operate (ATO) under the Federal Information Security Management Act of 2002 (FISMA) was issued on July 7, 2010. Continuous monitoring tests are conducted to ensure controls remain in place and reviews, updates, and adjustments are completed where appropriate, e.g., system processes and procedures, system policies, risk assessment, and contingency testing.

Operational Controls

As stated in the Research Support System Security Plan, all employees and contractors undergo a national agency check with inquiries (NACI) security check when employed or contracted. This involves a check of federal and local law enforcement records to ensure the trustworthiness of the employee. Initial and annual security awareness training with a section on data privacy is mandatory for all new and existing NOS staff as well as anyone who is authorized physical access to the information system. Training includes a section on Privacy Act information.

Access rights to all information on the Research Support System is controlled by group administration, which is defined by organizational components and then by roles. Although the system secures information through assigning a user a unique identifier and assigning that user to a group with restricted access, the user could still cut and paste information or copy information to a non-secure source. This type of activity is mitigated by the annual security training and, to protect mobile information, all NOS laptops are fully encrypted.

The NOAA6301 system is composed of multiple research facilities which provide research support for NOS, other NOAA and DOC offices as well as North Carolina, South Carolina and Maryland State government offices. Joint Partnership Agreements (JPAs), Memorandums of Agreement (MOAs) and Memorandums of Understanding (MOUs) are in place with each organizational entity that supports NOAA6301. In the case where data specific to educational outreach are shared with partners, it is expected

that they will have their own mandated requirements regarding the handling of privacy information that are consistent with those that apply to NOAA. The risk is mitigated by requiring any partner to take the NOAA annual privacy and security training. Partners' system access is controlled through NOAA6301.

Physical and environment controls for each facility managed by NCCOS are in place and compliant with Moderate control requirements as defined in NIST SP 800-53.

Technical Controls

Least privilege is applied when storing information and providing access to information (least privilege is the practice of granting the least amount of access possible to a user while still allowing fulfillment of job responsibilities. Groups are created to control the management of information access. Groups are determined by organizational components, e.g., NOS, NCCOS, and CCFHR, and then further defined by function and/or role, e.g., administrators, HR, project team). Authorized membership to groups is determined by the data owner, but managed by system administrators who have annual security role training requirements.

As an additional precaution, 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 purpose 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.”

Data Extract Log and Verify:

Currently the process for logging and monitoring data extracts is manual. Access to pertinent files or information is limited to system administrators, supervisors, grant review personnel, or human resources personnel as applicable. Individuals with access are advised on the requirement to destroy all data extracts once they are no longer needed. The PII handled by this system is considered low risk and electronic logging has not been implemented.

The NIST Special Publication 800-53 Revision 3 On-line Database contains the security controls for federal information systems and organizations in a database that allows users to easily browse and search the SP 800-53 controls. For the moderate impact Research Support System Security Plan (SSP), the audit control details for four security controls are as follow:

AU-2 Auditable Events

According to the DOC Information Technology Security Program Policy (ITSPP) and NOAA Information Technology Security Manual (ITSM), Research Support System records of auditable events are required. These two documents define the “organization-defined auditable events” to include:

- logon (successful and failed),
- remote connections,
- audit log failures,
- access violations account logon events,
- account management events,
- directory service access events,
- object access failures,
- policy change failures,
- privilege use failures, and
- system events.

All system components are configured to record their own events. This list is maintained in the Research Support System Security Plan and is reviewed and updated, as needed, on an annual basis. Data owners of PII records are advised to review records every 90 days to determine if they are to be disposed or retained for an additional amount of time. Enforcement of auditable events is configured during the build process for each device. Automated controls are implemented for auditing system components where applicable information resides. The Information System Security Officer (ISSO) and the NCCOS IT Manager periodically review and correct operational deficiencies to ensure compliance with security control procedures.

AU-3 Content of Audit Records

According to the DOC ITSPP, the Research Support System ensures the system components are configured to produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Research Support System components maintain their own set of logs with the exception of when a syslog server exists on-site in at which redirection of events to the server is accomplished at configuration.

A standard set of properties is recorded for each event:

- Date and time of event
- Program or component where the event occurred
- Type and level of event

- Subject identity
- Outcome of events

The Research Support System provides the capability for more detailed reporting to include additional, more detailed information in the audit records for audit events identified by type, location, or subject. Systems record this information and settings can be adjusted for detailed reporting as needed.

AU-6 Audit Review, Analysis, and Reporting

The Research Support System components are configured to log the specific auditable events identified above. System administrators in all Research Support System subsystems review their components' audit logs on a monthly basis. In addition, tools are in place to alert administrators of suspicious or notable activity.

A change auditor is currently configured to monitor critical changes to group policies, directory structure, permissions on select files/folders, login attempts on restricted accounts protecting the higher level components.

If and when activity is found that warrants investigation, the system administrator will begin notification of the appropriate security personnel as per NOAA-wide incident handling procedures.

AU-11 Audit Record Retention

The Research Support System is compliant with NOAA's and DOC's 180 day retention requirements. System components are configured to retain security logs to a maximum capacity or for a maximum length of time or both (whichever comes first) as long as 180 days is the minimum retention period. Once the configured maximum is reached, logs are overwritten.

All system inventory devices are set up and configured according to the Research Support System Configuration Management Plan and utilize Secure Configuration Templates. The Research Support System Security Plan is used as the authoritative guide for implementation of policy and minimum configuration requirements.

An exception to the 180 day rule is the need to review PII records every 90 days. Data owners of PII records are advised to review records every 90 days to determine if they are to be disposed or retained for an additional amount of time.

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.

The current Authorization to Operate (ATO) under the [Federal Information Security Management Act of 2002](#) (FISMA) is expected to be renewed by July 31, 2013.

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

No. The Research Support System does not require a separate system of records. The existing Privacy Act system of records notices (SORNs) for NOAA covers the personal information in this system. See the Federal Register's [Compilation](#) of Privacy Act Issuances for the current NOAA SORNs.

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

Chapters 1601 and 1607 of [NOAA's Records Schedules](#) provide supplemental record retention guidance for the NCCOS Research Support System. Chapter 1601 pertains to general administration for the National Ocean Service and Chapter 1607 pertains to specific records managed by the NCCOS Research Support System.

The applicable records schedule items from Chapter 1601 and 1607 follow:

1601-02 Grants Working Files (New Item) (N1- 370-02-5)

Copies of information maintained for each grant and award made to support National Ocean Service (NOS projects). The original information for Grant Files is maintained in the Grants Management Office. Files include, but are not limited to: copies of the general announcement; Federal Register Notice; applications, assurances, and certifications; correspondence; evaluations and review reports; information related to the proposal or award process; site visit documentation; proposal negotiations, recommendations, and revisions; and financial and budgetary reports, both periodic and final. Files are maintained in hard copy and arranged by fiscal year and grant number.

Authorized Disposition:

Record keeping paper copy: Destroy three years following the final financial status report.

1601-04 Electronic Copies (N1-370-02-5)

Word processing, spreadsheet, e-mail and other electronic copies used to create file copies of official records.

Authorized Disposition:

Destroy when file copy has been generated or no longer needed for reference.”

1601-05 NOS Annual Operating Plan (AOP) Information Tracking Systems (New Item) (N1-370-04-4)

This system is used for production of the fiscal year AOP and quarterly reporting on milestone progress. The system contains NOAA Goals and Objectives, NOS Goals and Objectives, NOS Performance Measures and Milestones, Significant Issues and Accomplishments.

Authorized Disposition:

1. *Information within the system (data)*: Cut off at the Fiscal Year. Destroy 3 years after cut off.
2. *System Documentation*: Destroy 6 months after system is terminated.
3. *System Inputs* (NOAA Strategic Plan, NOAA Implementation Plans, NOS Strategic Plan, Annual budget information, Program Office Strategic Plans, Program Office Annual plans (100-11 and 100-12)): Follow disposition instructions for related records.
4. *System Outputs* (AOP and other administrative reports (100-11 and 100-12)): Follow disposition instructions for related records.”

1601-07 Memorandum of Agreement (MOA) Tracking Systems (New Item) (N1-370-04-4)

This system is used to track the metadata of MOA, MOU (Memorandum of Understanding), and Interagency Agreements. The system includes metadata, which is used for tracking, cover sheet generation, and report generation.

Authorized Disposition:

1. *Information within the system (data)*: Cut off at the end of the calendar year. Destroy 3 years after cut off.
2. *System Documentation*: Destroy 6 months after system is terminated.
3. *System Inputs* (agreements (200-18)): Follow disposition instructions for related records.
4. *System Outputs* (multiple reports): Destroy when no longer needed for reference.

1607-04 Program Funding Database (New Item)

Database is used to track progress and provide quick access on Coastal Ocean Research grants, proposals, and project information. The system contains: the proposal number, program element, proposal title, principal investigator's name and other identifying information; proposal status; areas of research; reviewer reporting sheet and budget information.

Authorized Disposition:

1. *Information within the System (data)*: Destroy three years following submission of the Final Financial Status Report associated with completion of the entire research project.
2. *System Documentation*: Destroy 6 months after system is terminated.

3. *System Inputs* (Proposals received from research community (part of Grants Working File 0000-02); Internet; telephone book (100-04)): Follow disposition instructions for related records.

4. *System Outputs* (Printouts, Reports, Final Studies): Destroy 3 years after the calendar year in which the file was closed.