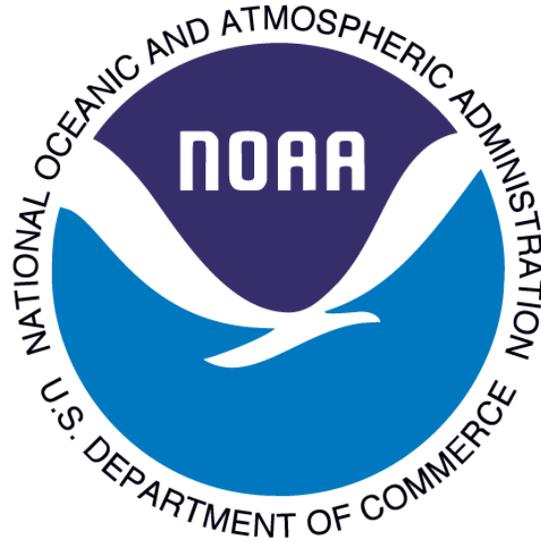


**U. S. Department of Commerce
National Oceanic and Atmospheric Administration**



**National Coastal Data Development Center Network
NOAA 5036**

PRIVACY IMPACT ASSESSMENT

January 17, 2013

Prepared by: Juanita Sandidge, NOAA5036 System Owner

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

National Coastal Data Development Center (NCDDC) Network

Unique Project Identifier:

OMB Exhibit 300 identification number - 006-48-01-13-01-3209-00

IT Security System: NOAA 5036 (NCDDC Local Area Network)

Project Description: The National Oceanic and Atmospheric Administration's (NOAA's) National Coastal Data Development Center (NCDDC) network is a General Support System (GSS). The mission of the NCDDC is to support ecosystem stewardship by providing access to the nation's coastal data resources. NCDDC is located at Stennis Space Center, Mississippi. A mirror site of NCDDC's public web presence to be used for Continuity of Operations (COOP) purposes has been established at NOAA's National Geophysical Data Center (NGDC) in Boulder, Colorado.

The NCDDC provides access to coastal data and metadata stored at various locations both internal and external to NOAA via its public web presence.

The NCDDC network consists of four separate components, an administrative local area network (LAN) component; a public access-mission support component; a staging component; and a mirror site component. Each of these components is deployed on separate subnets. The public support and mirror site components are the public presence of NCDDC. The staging component is used specifically for testing applications prior to deployment into the public. The administrative LAN component is used for the daily business of NCDDC including personnel, budget, application development, and other internal administrative matters.

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

Information collected from employees and contractors consists of names, addresses, social security numbers (SSNs), date of birth, and place of birth. SSNs, date of birth, and place of birth for employees and contractors are located on the LAN in an area accessible only by the Administrative Officer and system administration personnel. Names and addresses only of employees and contractors are located on the LAN in an area accessible by all employees. Information collected from collaboration partners (may be outside of NOAA) consists of their names and email addresses. Information gathered from the public via web Account Request Forms consists of names, email addresses and optionally organization, department/division, and telephone number.

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

Information is collected from employees and contractors to determine eligibility for system authentication into access controlled sites/applications; to provide the public with a point of contact within the organization; and to provide a means to contact employees in emergency situations and for internal center administrative purposes, i.e. to request security clearances, to request NASA Stennis site badges, and to request Common Access Cards. Information is collected from collaboration partners for communication purposes

only. Information is collected from the public, as described in Question 1, for system account creation and communication with the account requestor only.

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

The information, names, addresses and email addresses, collected from employees, contractors, and the public is used to manage account information for access control to systems and web applications; names and email addresses of employees and contractors are used to direct the public to appropriate personnel within the organization; and for emergency, disaster recovery, and continuity of operations. Names, addresses, SSNs, place of birth, and date of birth are used for coordination with regional security offices for clearances and coordination with NASA for site badging purposes. NCDDC is a tenant on a NASA facility and is required to have NASA badges for entrance to the site.

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

The information used for account management is not shared with anyone. Federal and contractor employee names and email addresses that are published on the NCDDC Web site are available to the public. Emergency contact information is shared internally in NOAA only, as is the information used for continuity of operations. Names, addresses, SSNs, place of birth, and date of birth are shared with the NOAA security office for clearance investigation purposes as well as being shared with NASA security for site badging purposes.

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?

Individual federal employees and contractors are required to provide the information as a condition of employment. The information is required for the effective administration of the center, including continuity of operations in case of an emergency. Individuals are provided an explanation for why the information must be provided and links to the NOAA privacy policy are provided.

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

Management Controls

Access control procedures are in place for all account management sites and all user files, as described in the NOAA5036 Certification and Accreditation (C&A) required for the network to commence operations. For information retained for Center administrative purposes, access controls ensure that only the Administrative Officer and approved system administrators have access to this information. System administration personnel

may not access files without the permission of the file owner or an appropriate federal employee (the Administrative Officer, Center Director, System Owner, or Contract Officer Representative).

All personnel with access to any of these types of files are trained on the handling of personally identifiable information (PII) in electronic and paper form. Also, use of encrypted e-mail containing PII is required of all employees and training is provided.

Operational Controls

Auditing of accounts containing information used to determine eligibility for authentication into access controlled sites/applications is done on an annual basis. No auditing is done on information provided to the public. For all other accounts containing PII, logging of file access is in place, and auditing of access to this folder is done at least monthly.

Technical Controls

Access to information used for authentication is available only via authenticated access to the system. The system is maintained in accordance with the Assessment and Accreditation documentation provided. No authentication is required for access to public information including the names of individuals within the organization used as points of contact for business purposes. Access to employee emergency contact information is available to all authenticated users in the NCDDC Network, except to guest users which are explicitly denied access. Network and physical controls are in place to ensure that PII and internal administrative information can be accessed only by authorized personnel.

Access to the NASA badging system requires an authenticated username and password. Access to this system is limited by NASA. Users are vetted by NASA security and required to complete PII training through NASA before being issued an account on NASA's system. NASA adheres to the controls outlined in the [Federal Information Security Management Act of 2002](#) (FISMA).

Data Extract Log and Verify Requirement

Logging/monitoring system access is done using the Varonis DatAdvantage application. This application maintains a record of file access by users and user access by files. Auditable events for files include creation, open, rename, edit, delete, change of access controls, and move. The content of audit records includes user name, timestamp, file name, and length of time file is in use. Monitoring is done at least monthly; logs are retained on backup tape for one year. Additionally, file inactivity is monitored to ensure that PII within the system is required for business operations. PII within this system is not extracted, but is used within these files.

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 this system on November 8, 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. An annual Risk Management Framework Assessment and Authorization was completed on November 15, 2012 for reaffirmation of the NOAA5036 authority to operate (ATO).

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. Existing Privacy Act system of records notices (SORNs) for NOAA cover the personal information in this system: COMMERCE/DEPT-18 - Employees Personnel Files Not Covered By Notices of Other Agencies and NOAA-11 – NOAA Mailing Lists, would apply. The NOAA Mailing Lists is currently under revision by the NOAA Privacy Officer.

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. The underlying paper records relating to employees are covered by GRS 1, Civilian Personnel Records.

In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal under other records schedules 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.

Guidance for these records in the NOAA Records Schedules refers disposition to GRS 20.

System Contact:

Juanita Sandidge

System Owner

(228) 688-4812

Juanita.Sandidge@noaa.gov