

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



**National Climatic Data Center LAN
NOAA5009**

PRIVACY IMPACT ASSESSMENT

February 22, 2012

Prepared by: Jennifer Urzen, NCDC Information Systems Security Officer
Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer

National Climatic Data Center Local Area Network

Unique Project Identifier: 006-48-00-00-01-3209-00-108-023
(NOAA National Data Systems)

Project Description:

NCDC is the official data management entity for meteorological and climatological information in the United States, with additional global data management commitments defined by international agreement and scientific need. Its core responsibility is to ensure secure storage and scientific data stewardship of its holdings, including both remotely- and directly-sensed climate data records including related and derived environmental information.

The National Environmental Satellite, Data and Information Service (NESDIS) E-Commerce System (NeS2) handles customer order payment processing for the data centers listed below, both online (via the Online Store:

<http://ols.nndc.noaa.gov/plolstore/plsql/olstore.main?look=1>) and offline (via direct interaction between customers and internal customer service representatives). NeS2 is hosted on the NCDC Local Area Network, NOAA 5009. NCDC hosts the customer data for all three data centers.

NeS2 handles the product inventory, customer tracking for billing and shipping, accounting/fiscal processing, and reporting for the three NOAA National Data Centers:

- 1) National Climatic Data Center (NCDC): NCDC is the world's largest active archive of weather data.
- 2) National Geophysical Data Center (NGDC): NGDC provides stewardship, products, and services for geophysical data describing the solid earth, marine, and solar-terrestrial environment, as well as earth observations from space.
- 3) National Oceanographic Data Center (NODC): NODC archives & provides public access to global oceanographic and coastal data, products, and information.

Also, NCDC has several shared folders on its Active Directory domain that contain personnel performance appraisals.

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

In addition to archived weather data:

- a) The information collected in NES2 from a customer when placing an order consists of the customer's name, billing address, phone number, and credit card number and expiration date, by which NCDC can bill for its products and services. The customer may place an order to NCDC, NODC, or NGDC and provide the information over the Internet using the NCDC Online Ordering System, by facsimile, by surface mail, or over the phone.

This information provided by the customer is the only personally identifiable information (PII) associated with these three data centers. The NeS2 system is hosted by NCDC. NGDC and NODC access customer orders from NCDC via an SSL Web interface. The information collected in NES2 from a customer when placing an order consists of the customer's name, billing address, phone number, and credit card number and expiration date, by which NCDC can bill for its products and services. The customer may place an order to NCDC, NODC, or NGDC and provide the information over the Internet using the NCDC Online Ordering System, by facsimile, by surface mail, or over the phone. This information provided by the customer is the only personally identifiable information (PII) associated with these three data centers. The NeS2 system is hosted by NCDC. NGDC and NODC access customer orders from NCDC via an SSL Web interface. The credit card information is collected and stored at [Pay.gov](https://www.pay.gov). This system is managed by the United States (U.S.) Treasury and is required to be used by all federal agencies who offer services/products by credit card payment. All credit card information including number, name, and address is stored and maintained by Pay.gov. NCDC does not store any of this financial information.

- b) The following information is collected in each performance plan and appraisal:
- Employee's name
 - Dates for the period of performance
 - Title, Series, and Grade of the position
 - Employee's Division (where assigned)
 - Information about the employee's work and work performance, constituting the plan or appraisal

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

- a) The customer information collected is needed by NCDC, NGDC, and NODC customer service employees to fill, cancel, or void orders and issue refunds when necessary in NES2.
- b) The performance appraisal information is collected in order to assure employees are performing according to the terms of their written performance plan.

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

- a) The information collected in NES2 is used by NCDC, NGDC, and NODC customer service employees to carry out the processes described in Question 2 above. There are no other uses of the data.
- b) The performance appraisal assists in providing Federal Government performance goals to define the level of performance to be achieved during the year in which the plan is submitted.

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

- a) Customer information is used solely for the processing of customer orders, and is shared only with employees that need to know the information, namely customer service employees for NCDC, NGDC, and NODC. The information is never shared

with third parties. NeS2 uses Pay.gov, which is hosted by the Treasury Department. It is a secure government-wide portal that provides electronic payment capabilities for federal agencies and their customers, both public and private. Pay.gov receives the individual customer's information via a Secure Socket Layer (SSL) connection, in order to charge for the order. SSL is a secure technology used to encrypt information from an individual's computer to a Web site when performing transactions over the Internet. A Web address that starts with *https://* indicates that an SSL connection is being used.

Under the provisions of the Privacy Act, individual customer information (name of individual, address, phone number, and credit card or other account information), is not shared except as described above and as otherwise permitted by the Privacy Act itself. Should a Freedom of Information Act (FOIA) request be received, information would only be released if the FOIA required release.

In the case of a FOIA request for information about orders from a business, only the business name, address, and phone number would be released. Account information and the name of the contact at the business are not provided unless required by the FOIA.

- b) The performance plan information is shared only with other management and administrative support personnel, as required.

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?

- a) This statement appears at the bottom of each Web page in NES2:

“By sending us an electronic mail message, you may be sending us personal information (e.g., name, address, E-mail address). We may store the name and address of the requester in order to respond to the request or to otherwise resolve the subject matter of your E-mail. If you order weather data, we will enter the information you submit into our electronic database. This information will be used to fill your request and ship your data. In limited circumstances, including the [Freedom of Information Act \(FOIA\)](#), we may be required by law to disclose information you submit. We recommend that you do not use E-mail to submit credit card information to NCDC. Visit [NCDC Security Issues](#) to learn more about credit card security on our Web site.

This privacy policy has been developed to comply with the requirement in Section 208 of the E-Government Act of 2002 (44 U.S.C. 3501 note) and the Department of Commerce IT Privacy Policy.”

Providing this information does not constitute a collection of information within the meaning of the Paperwork Reduction Act (PRA), and approval by the Office of Management and Budget (OMB) is not required.

- b) Performance plans are a mandatory item; thus, declining to provide information is not applicable. .

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

Management Controls

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. Every The IT system undergoes a continuous Assessment and Accreditation (A&A) process that is performed by a contractor company. 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. System security checks have to be performed regularly and reported to NESDIS Headquarters on a periodic schedule.

Operational Controls

The NCDC data center where the servers are located is a facility staffed 24 hours a day, seven days a week with uniformed security guards. The computer room has a keycode entry system and is also staffed with computer operators 24 hours a day, seven days a week. Visitors and maintenance contractors must sign in at the guard desk, sign in upon entering and leaving the computer room, and be escorted at all times within the computer room. Data backup is performed daily, and the backup data is stored in a secure offsite location that only a limited number of people are allowed to enter. The backup facility also has a keycode entry. These controls apply to the customer order data from NGDC and NODC, which is hosted on the NCDC site.

Technical Controls

NCDC employs host-based and network Intrusion Detection Systems to help ensure that the systems containing customer information are not accessed by unauthorized users. Customer information is encrypted except when it is needed and being used by a customer service employee, who accesses the information using an encrypted connection. Specific IP addresses from NODC and NGDC are allowed access to the customer database at NCDC via the encrypted Web interface.

Customer service employees must be assigned and enter a user ID and password to access customer information. Remote administration of the database and servers is performed over encrypted channels, and only specially approved users that need access to the servers are allowed to log in. Backups are performed on a daily basis and the customer information is kept encrypted on all backups.

Oracle database roles are used to assign user privileges, with privileges authorized by the system supervisor. The principle of least access is applied for access to all resources. The system provides for user roles assigned by administrative staff. A written protocol for authorizing, managing, and logging access is part of the system development. Data changes to the system are tracked and record who makes changes to the data, the date and time of the changes, and what the change was.

General policies for the use of Oracle roles to access data stored in the NeS2 database:

- Roles are created by the Oracle DBA in response to requests by application developers or the Data Management staff. Privileges such as Read, Update, Insert and Delete are granted to the roles based on the application's requirements.
- With the Data Owner's permission (verified by the Data Manager), roles are granted to users. Read roles are granted by the Data Manager. Admin and Insert/Update roles must be granted by the DBA.
- If the data is confidential, an agreement describing appropriate use of the data must be signed and on file with Data Management.
- Roles are *enabled* at the time the application is accessed and *disabled* when the user leaves the application. (An exception exists when users are granted read access to data via an ODBC connection (e.g., Crystal Reports, MS-Access)). This access requires a direct grant of the Select privilege on the object to the user.
- If time limits were set, roles are revoked from users when the privilege to use the data has expired.

Performance Plans on shared drives must be accessed by CAC Authentication, and principal of least privilege is used on the shared drives. More on performance plan policies below:

General policies for the performance plans being stored on shared drives:

- Principal of Least privilege is invoked by giving access to only those users who need to view the documents.
- If an account is required to be added to be able to view the plans, it must first go through the owner of the folder for approval.
- Write access is given only to those employees who are authorized to make changes. All others have read-only access.

Data Extract Logging and Verifying:

General policies for auditing Oracle production data and database usage include the following data extract logging and verifying controls:

- All data tables are constructed with four audit columns: a) created by; b) create date; c) last modified by; and d) last modified date. This feature ensures that a log entry is recorded whenever a new record is created or updated and by whom.
- History tables exist for active data tables. In addition to logging new record inserts and updates of existing records, the history tables record date and time of the change, the user making the change, and the nature of the change (i.e., old data and new data).
- Database auditing is activated for production databases. (e.g., logons, failed logons, deletes, table alterations), and logs are checked daily with automated scripts that notify administrators of potential violations.
- Users log on using individual accounts with passwords (not shared accounts).

The customer PII data is not extracted to other sources (i.e., print outs, reports, etc). The information is entered directly at the pay.gov website so that they can charge the card when the order is complete. Credit card information is not maintained in the NeS2 system at any time. It is stored solely at Pay.gov. See above, "General policies for the use of Oracle roles," regarding protection of access and use of the data.

One identified risk is the inadvertent release of private information to unauthorized staff because the system is used in an open office setting. This risk is mitigated by the development and issuance to users of written policies and procedures regarding their responsibilities to safeguard the sensitive personal information in the system. User responsibilities are reinforced by training when an individual is initially granted access to the system and periodically thereafter.

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 8/2012. The most recent controls testing was done for reaffirmation of the PIA in 8/2012.

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 for [DEPT-2, Accounts Receivable](#) and [DEPT-18, Employees Personnel Files Not Covered By Notices of Other Agencies](#) , apply to the personal information in this system.

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

For NES2, the retention period for these records is guided by the [NOAA/NESDIS Records Schedules](#). This system handles order information for climatological, geophysical, or oceanographic data held at any of the NOAA National Data Centers (NNDC). The system currently within use is the Customer Order Management Processing System (COMPS). Below are the requirements for record retention.

A. System Inputs:

1. Requests and orders for the various data products within the NNDC. These requests can be electronic (email or web-based), paper (letters or faxes), or telephonic.

Authorized Disposition:

Cut-off at end of quarter in which order/request has been completed.

Destroy/delete 6 months after cutoff (or longer if NOAA needs the information for audit purposes).

B. System Content:

1. Customer Information. Information, such as name, address and telephone number, on customers requesting data from the NNDC.

Authorized Disposition:

Cut-off when the last order is place by the customer. Delete 6 years and 3 months after cutoff or when no longer needed for marketing or reference purposes, whichever is later.

2. Product Catalog Information. This module contains information, such as pricing, media, keywords, descriptions, etc, concerning the various data products available.

Authorized Disposition:

Cut-off at the end of the calendar year when product description is superseded or product is obsolete. Delete when the information is no longer required for reference and/or reporting functions,(at least 6 years and 3 months after cut-off.)

3. **Financial Information:** This module contains the method of payment, credit card number verification and payment information, and similar information for each request of data.
Authorized Disposition:
Cut-off at the end of the fiscal year in which the purchase is made. Delete 6 years and 3 months after cut-off.
4. **Marketing Information:** This module contains the names, interests and contact information of customers signed up to receive new product announcements.
Authorized Disposition:
Cut-off data when superseded or no longer needed for marketing and/or reference. Delete immediately upon cut-off.

C. System Outputs

1. **Reports:** Reports and summaries showing customer satisfaction and a variety of performance statistics.
Authorized Disposition:
Cut-off when no longer needed for reporting and/or reference. Destroy immediately upon cut-off.
2. **Shipping information:** Work orders, transmittals and packing slips are printed from the system.
Authorized Disposition:
Cut-off when no longer need for reference or reporting. Destroy 6 months after cutoff.

D. System Documentation

1. **Information relating to the development and functionality of the system.** This includes any testing procedures, quality checking guidelines, government or contractor created manuals and handbooks, and other related materials.
Authorized Disposition:
Cut-off when the system is superseded or obsolete. Destroy 6 years 3 months after cut-off.

E. System Backup:

1. **Duplicate copy of system content kept to prevent loss of data in the event of a system crash.**
Authorized Disposition:
Cut-off when superseded by two subsequent backups. Delete immediately upon cut-off.

For the Performance Reviews, the electronic records, which are stored in the shared folder on the Windows network, are not the official record copy. The official record copy is printed and signed by all involved and filed in the employee's hard copy personnel file. The electronic version of the performance plan is retained until the employee no longer works for NCDC.