National Oceanic and Atmospheric Administration (NOAA)

National Environmental Satellite, Data and Information Service (NESDIS)

NESDIS E-Commerce System (NeS)

NeS Privacy Impact Assessment Statement

July 2008

Prepared by: Duane Dunston, NCDC Information System Security Officer

Reviewed by: Sarah Brabson, NOAA OCIO

NESDIS E-Commerce System (NeS)

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

IT Security System: NOAA 5009 (NCDC Local Area Network)

Project Description

The National Environmental Satellite, Data and Information Service (NESDIS) E-Commerce System (NeS) handles customer order payment processing for the data centers listed below, both online (via the Online Store: http://www.ncdc.noaa.gov/oa/nolos/oluser.html) and offline (via direct interaction between customers and internal customer service representatives). NeS is hosted on the NCDC Local Area Network, NOAA 5009. NCDC hosts the customer data for all three data centers.

NeS 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.

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

The information collected from a customer when placing an order includes the customer's name, billing address, phone number, and credit card number and expiration date, or "open account" information 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 associated with these three data centers. The NeS system is hosted by NCDC. NGDC and NODC access customer orders from NCDC via an SSL Web interface.

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

The information collected is needed by NCDC, NGDC, and NODC customer service

employees to fill, cancel, or void orders and issue refunds when necessary.

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

The information collected is needed by NCDC, NGDC, and NODC customer service employees to fill, cancel, or void orders and issue refunds when necessary.

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

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. NeS uses Pay.gov, which is hosted by the Treasury Department. It is a secure governmentwide 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 exempt from release in response to a Freedom of Information Act (FOIA) request, should one be received.

In the case of a Freedom of Information Act (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.

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 can individuals grant consent?

This statement appears at the bottom of each Web page:

"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. 36) 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.

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

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.

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 three years, the IT system undergoes a thorough Certification and Accreditation (C&A) process that is performed by a contractor company. The C&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.

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. Developers for NeS use test systems that do not contain customer information. 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 NeS 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.

A Security Certification and Accreditation (C&A) for the NeS (covering procedures for customer data from all three data centers) in accordance with the requirements of the Federal Information Security Act of 2002 (FISMA) was completed and is current. 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 IT system Security Plan has also been developed and is in effect.

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 transferred to Pay.gov so that they can charge the card when the order is complete. Credit card information is not maintained in the NeS system after the order is complete, nor is this information displayed in any other source outside the system. 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.

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, applies to the personal information in this system.

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. 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. GRS 6, item 1 authorizes the disposal of the equivalent paper copies six years and three months after the period covered by the account, **EXCEPT:** Accounts and supporting documents pertaining to American Indians are not authorized for disposal. Such records must be retained indefinitely since they may be needed in litigation involving the Government's role as trustee of property held by the Government and managed for the benefit of Indians.