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

National Environmental Satellite Data and Information Service (NESDIS)

Environmental Satellite Processing Center (ESPC)
NOAA 5045

PRIVACY IMPACT ASSESSMENT

June 27, 2013

Prepared by: Cordell B Robinson Security Specialist III GNS Inc Contractor Supporting Environmental Satellite Processing Center (ESPC) NOAA/NESDIS
Reviewed by: Sarah D. Brabson, NOAA Office of the Chief Information Officer

DOCUMENT CHANGE HISTORY

DOCUMENT REVISION LOG

The Document Revision Log identifies the series of revision to the Privacy Impact Assessment since the baseline release. This page will become a permanent part of this document.

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes Made by Name/Title/ Organization
1.0	05/2012	Initial Document	All	Cordell B. Robinson/SSIII/ESPC Contractor
2.0	01/2013	Final revisions per NOAA OCIO review	All	Cordell B. Robinson/SSIII/ESPC Contractor
3.0	06/2013	Insertion of impact level and update re ATO	Question 6	Sarah Brabson

NOAA/NESDIS Environmental Satellite Processing Center (ESPC) (NOAA5045) includes the following subsystems and minor application components:

- National Polar-orbiting Operational Environmental Satellite System (NPOESS) Preparatory Program (NPP) Data Exploitation (NDE) capability
- ESPC Critical Infrastructure Protection (CIP) capability
- Environmental Satellite Processing & Distribution System (ESPDS) Development capability (under contract to Solers, Inc.)
- Group on Earth Observation Network Broadcast (GEONETCAST) Americas (contractor-operated capability)

Unique Project Identifier: 006-48-01-16-01-3213-00

IT Security System: NOAA5045 Environmental Satellite Processing Center (ESPC)
System Owner: Linda Stathoplos
Deputy Manager, Mission Operations Division
NOAA/NESDIS/ Office of Satellite and Product Operations
National Environmental Satellite and Data Information Service
(301) 817-4000

Project Description:
The National Oceanic and Atmospheric Administration's (NOAA's) Environmental Satellite Processing Center (ESPC) is a government-owned Major Application sponsored by the Department of Commerce (DOC). NOAA's mission is to understand and predict changes in the Earth's environment and to conserve and manage coastal and marine resources to meet the nation's economic, social, and environmental needs. In support of that mission, the National Environmental Satellite Data, and Information Service (NESDIS) openly supplies environmental satellite data to users who request it. This is done without reservation, per international agreement, with the World Meteorological Organization.

Within NESDIS, the Office of Satellite and Product Operations (OSPO) manages the Environmental Satellite Processing Center (ESPC), a centralized processing system for the creation of environmental satellite data products and the distribution of environmental satellite data. ESPC relies on several distribution mechanisms to provide products and other data to users outside the OSPO organizational boundaries; these external users request access to the data through account management processes that involve the collection and use of non-sensitive personally identifiable information (PII): name, employment email address, employment telephone number, and employment physical address.

An example of how ESPC components use non-sensitive PII is the Group on Earth Observations Network Broadcast (GEONETCAST)-Americas (GNC-A) subsystem, which became operational in April 2008. The GNC-A subsystem relies on commercial satellite operators to broadcast environmental information to users in the Western Hemisphere. Data users include anyone within the satellite footprint who has the

equipment to receive the broadcast. Data providers include ESPC itself, other U.S. federal agencies, academic partners, and international government agencies. Users who wish to access information distributed via GNC-A register with the GNC-A program manager through a form available on the GNC-A web site. Data providers who wish to distribute their information via GNC-A must register with the program manager, using a separate form with the same PII elements. Other ESPC distribution components collect similar non-sensitive PII to organize and manage user accounts.

1. What information is to be collected (e.g., nature and source)?
ESPC account management processes typically collect name, address, phone number, and email address from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms, or email.

2. Why is the information being collected (e.g., to determine eligibility)?
The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.

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

The intended use of the information is to verify the accuracy of the user or supplier's request, and the legitimacy of the provider's organization.

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

The collected information is not normally shared outside NOAA. The information can be shared with law enforcement or information security incident response teams in support of their duties.

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?

Individuals provide the information on a voluntary basis, and may decline to provide the information requested. If they decline to provide the requested information, they will still be able to received ESPC products generally available to all users; however, they may not be able to receive specifically requested products.

If a provider declines to provide the requested information, they will not be able to supply products for use by ESPC, including retransmission via the GNC-A subsystem or other distribution components.

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

Because NOAA5045 is a federal information system managed within an Executive branch agency, the information belonging to NOAA5045 is governed by the guidance published by the National Institute of Standards and Technology (NIST), specifically in NIST Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems. As noted in FIPS 200, the minimum security requirements "represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems."

Account management information for ESPC components is considered within the security accreditation boundary (*Accreditation boundary refers to the physical, logical, administrative, and/or managerial perimeter into which the IT elements of an information system are gathered for security review purposes*). Since NOAA5045 is used to support its operational activities, typically, account management information is organized in standard office automation documents and/or spreadsheets, which reside on the government workstations, used by the ESPC government and contractor staff. These workstations generally fall within the accreditation boundary of NOAA5044, National Satellite Operations Facility (NSOF) Administrative Local Area Network.

For GNC-A, the file is normally password-protected, and the password is known only to the Program Manager (PM) and the System Administrator (SA). The password-protected file will be backed up to the PM and SA personal network drive, also within the accreditation boundary for NOAA5044.

Management Controls

The information covered under this PIA falls within the accreditation boundary for NOAA5045, and relies on NOAA5045 Management controls, as described in the NOAA5045 System Security Plan. NIST guidance identifies 5 management control families with 28 individual management controls within the control families in the areas of certification, accreditation, and security assessments; security planning; risk assessment; and systems and services acquisition. The most recent security assessment for NOAA5045, conducted in March 2011, identified 12 of these individual controls as requiring some level of remediation to bring the control to full implementation status. Ongoing efforts within the management of NOAA5045 include several security improvement projects and other tasks and activities to address the current deficiencies, which are expected to be fully remediated by the end of FY2012. None of the deficiencies noted undermine the Confidentiality of the information covered under this PIA.

Operational Controls
The information covered under this PIA is stored on workstations and servers within the accreditation boundary of CITS LAN NOAA5044, and relies on the operational controls of NOAA5044 for security as described in the NOAA5044 System Security Plan. NIST guidance identifies nine operational control families with 79 individual operational controls within the control families in the areas of Awareness and Training, Configuration Management, Contingency Planning, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, Personnel Security, and System and Information Integrity.

Technical Controls

This is a high impact system.

Account management data is not extracted from the documents where it resides, so no logging of extracts is required. No automated process exists or is required.

ESPC has completed the Security Authorization process as required by the Federal Information Security Act of 2002 (FISMA), with Authorization To Operate (ATO) as of April 14, 2013. This process is an audit of policies, procedures, controls, and contingency planning, with continuous monitoring, and reauthorization annually.

ESPC adheres to the NOAA Continuous Monitoring policy for all NOAA IT systems. The policy documents the requirement for an annual assessment of the effectiveness of the security controls. The first planned annual authorization is scheduled for completion on April 14, 2014.

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

The applicable System of Records t is NOAA 11 NOAA Mailing Lists which is maintained at numerous NOAA installations, one being National Earth Satellite Service in Suitland, Md. Currently the NOAA11 SORN is in the process of being updated.

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

Yes, ESPC, as a NESDIS system, is covered under records control schedule N1-370-03-10, dated July 2005, which is available at:

http://www.corporateservices.noaa.gov/audit/records_management/schedules/chapter-1400-satellites-and-data-centers.pdf.