Version Number: 01-2015

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

Privacy Impact Assessment for the
National Environmental Satellite Data and Information Service (NESDIS)
Environmental Satellite Processing Center (ESPC)
NOAA5045

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.06.08 13:16:31 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment

NOAA/NESDIS Environmental Satellite Processing Center (ESPC) (NOAA5045)

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

Introduction: System 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) and operated by NOAA within the National Environmental Satellite Data and Information Service (NESDIS). NOAA's mission of Science, Service and Stewardship is to understand and predict changes in the climate, weather, oceans, and coasts, to share that knowledge and information with others, and to conserve and manage coastal and marine ecosystems and resources. NESDIS openly supplies environmental satellite data to users in all governments that request it. This is done without reservation, per international agreement with the World Meteorological Organization. The data processed by the ESPC is used to develop products that are used to analyze environmental conditions and to predict physical and climatological changes. ESPC data is used by 200-300 identified users such as various governments, educational institutions, research entities and individuals. There are many more unidentified users accessing data through the internet.

ESPC is NOAA's primary data-processing systems for the nation's environmental satellite data. ESPC is managed by the Office of Satellite and Product Operations (OSPO) within NOAA, and is the world's largest civil operational environmental space organization. ESPC's operational components are located at the NOAA Satellite Operations Facility (NSOF) in Suitland, Maryland; the NOAA Center for Weather and Climate Prediction (NCWCP), College Park, Maryland; Wallops Station, Wallops Island, Virginia; and Fairmont, West Virginia. ESPC also has information and system components at other NOAA facilities in Silver Spring, Maryland. OSPO manages and directs the operation of the central ground facilities for ESPC that ingest, process, and distribute environmental satellite data and derived products to domestic and foreign users.

ESPC is 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. ESPC account management processes typically collect name, address, phone number, and email address from individuals or organizations wishing to access or provide ESPC data via its distribution mechanisms. This information is voluntarily submitted through the use of online forms or a form attached to an email. This information is stored in NOAA5044, NSOF LAN and only the information needed to create the account is stored in NOAA5045. These forms are implemented in accordance with the NOAA/NESDIS policy for *Access and Distribution of Environmental Satellite Data and Products,* February 17, 2011. The *ESPC Data Access Request Form and Data Submission Form* and the NOAA/NESDIS policy are available at: http://www.ospo.noaa.gov/Organization/About/access.html.

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 also register with the program manager, using a separate form. Other ESPC distribution components collect similar non-sensitive PII to organize and manage user accounts.

Information sharing: This information is not shared outside the system.

Authority: 5 U.S.C 301 is a general authority for conducting the Department's business. Additional authority from NOAA-11: 15 U.S.C. 1512, Powers and duties of Department.

The Security Categorization of NOAA5045 has been determined using the guidance in FIPS 199 and NIST SP 800-60. Legislative mandate requires that NOAA provide environmental monitoring, assessment, and prediction services to the U.S. Public in order to perform its core mission to protect life and property of U.S. citizens. ESPC (NOAA5045) has been designated as a National-Critical system under Presidential Decision Directive/NSC-63 (PDD-63). *The designation of the system's overall security categorization is high*. This categorization is based on categorization of the individual security objectives as Confidentiality-Moderate, Integrity-High, and Availability-High.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

__X__ This is an existing information system with no changes that create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): Though employment contact information is preferred, a customer or supplier of data could submit their home address, telephone number and/or email address on the form.					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	X	Online	X
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): NESDIS openly supplies environmental satellite data to users in all governments that request it. This is done without reservation, per international agreement with the World Meteorological Organization.					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): NESDIS openly supplies environmental satellite data to users in all governments and academic partners that request it. This is done without reservation, per international agreement with the World Meteorological Organization.					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

NESDIS openly supplies environmental satellite data to users in all governments or academic institutions that 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, email address, telephone number, and physical address.

External users are federal employees/contractors, members of the public, governments, and academic institutions both domestic and foreign. ESPC customers and data providers voluntarily submit non-sensitive personally identifiable information (PII): their name and

contact information via an account request form. No PII is included with the data from data providers, when uploaded into the system.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

X	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: Contact information is collected from NOAA5044 for creating an account on ESPC and the technical controls to prevent PII/BII leakage are firewall ACLs, IDS and malware protection.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public*	X	Government Employees	X
Contractors	X		
Other (specify):			

*Account information is not shared with the public.

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.ospo.noaa.gov/Organization/About/access.html. _____.	
X	Yes, notice is provided by other means.	Specify how: If individuals require an account, they visit the ESPC website and download the form required or contact the ESPC Help Desk and the form is emailed. Data requestors and data providers voluntarily submit their name and contact information via the account request form. This form is implemented in accordance with the NOAA/NESDIS policy for Access and Distribution of Environmental Satellite Data and Products, February 17, 2011. The ESPC Data Access Request Form, Version 15, April 2016, and the NOAA/NESDIS policy are available at: http://www.ospo.noaa.gov/Organization/About/access.html.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: If individuals require an account, then they voluntarily submit their name and contact information via an account request form. Otherwise, they do not provide their information. If they decline, they will not be able to have an account.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: If individuals require an account, they voluntarily submit their name and contact information via an account request form. There is only one use for the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: If individuals require an account update, they contact the ESPC Help Desk and voluntarily submit their updated contact information via an account request form.
	No, individuals do not have an opportunity to review/update PII/BII	Specify why not:

	pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Contact information is stored on the NSOF ADMIN LAN (NOAA5044) and access to the forms are monitored, tracked and recorded through NSOF ADMIN LAN mechanisms. If someone that does not have access and attempts to access to a folder containing PII/BII, a failed access log is created. We also employ security monitoring tools that can detect PII in unauthorized locations.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): October 14,2016. ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM). ESPC POA&M 68433 is tracking PL-5.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

ESPC has NIST 800-53 Rev 4 security controls in place, including, but not limited to: Separation of duties, access controls, encryption in transit, training, and auditing.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Chapter 100 – General, Chapter 200 – Administrative and Housekeeping Records, and Chapter 300 – Personnel.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:

X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified based on the PII stored.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Contact information is stored on the NSOF ADMIN LAN (NOAA5044) and access to the forms are monitored, tracked and recorded through NSOF ADMIN LAN mechanisms. If someone that does not have access attempts to access a folder containing PII/BII, a failed access log is created. We also employ security monitoring tools that can detect PII in unauthorized locations.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: A Privacy Act Statement has been added on the OSPO Web site.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.