Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
Data Collection System (DCS)
NOAA5004

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

12/13/2019

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA DCS

Unique Project Identifier: NOAA5004 (not affiliated with an Exhibit 300).

Introduction: System Description

The Wallops Command and Data Acquisition Station (WCDAS) is the direct link to the Geosynchronous Operational Environmental Satellites (GOES) and the Polar Operational Environmental Satellites (POES) that collect the Nation's weather data. The primary Data Collection System (DCS) for the NOAA5004 LAN is located within the WCDAS facility. A backup DCS will be located at the NOAA Satellite Operations Facility (NSOF).

The DCS is a data relay system which enables a large variety of environmental data to be gathered from point sources or Data Collection Platforms (DCP). The purpose of the DCS is to collect data from the government sponsored and government-owned DCPs and disseminate the data to all users of the DCS service. The DCS collects data from DCPs located throughout the hemisphere that are either part of or sponsored by a government agency. DCPs include terrestrial, airborne and tethered platforms measuring such observations as wind speed, wave height, water depth, temperature, etc. Users provide their own DCPs with sensors measuring conditions of interest to them. For example, water height data is of interest to flood management, while wind speed and direction are of interest to aviation and wildfire management, etc. The DCP transmits its collected data to, and through, the GOES spacecraft to the DCS Systems located within the WCDAS and the NSOF.

The DCS processes and logs data from the DCPs and distributes the data to registered users (federal, state and local agencies). The DCS distributes data via a domestic satellite (DOMSAT) direct broadcast circuit. The system also automatically transmits selected DCP data to National Weather Service (NWS) users via the Internet and the National Weather Service Telecommunications Gateway (NWSTG). Many other users access the data through the Internet. In order to meet regulatory requirements for the GOES DCS, NOAA requests some contact information and a question about Data use, and whether they are government (foreign, federal, state, local or tribal, or non-government (public or private agencies) operating the observing system or using its data), in order to judge if they qualify for system use, which is restricted by law to government or *government-sponsored* environmental use. That information is submitted online through the GOES DCS NOAA5004 system. An agency makes a request for a System Use Agreement (SUA) through online submission of a form approved under OMB Control No. 0648-0157. On that form, NOAA requests contact information for up to 3 individuals who are signers and users of data. Once an agency has been authorized for use of the GOES DCS, through the submission of the SUA request, NOAA requests information that is relevant to either an agency's access to NOAA's satellites, or relevant to access to NOAA's IT systems; that is, information needed to provide a system login. That community of users is not the general public. The agency identifies to NOAA whom they wish to use as those contact points. No user is required to provide information unless the agency has delegated job related responsibilities to that user. NOAA requires those contact points in order to carry out responsibilities related to access to NOAA's IT systems, or access to NOAA's satellites (i.e, whom to contact if a transmitter is interfering with another user.)

NOAA also collects information through the IT System for NOAA5004 through a survey form approved under OMB Control No. 0648-0227, from users of NOAA weather satellite data (any of the same categories as may register to use the GOES DCS) , including those who do not have satellite ground stations. NOAA has entered into agreements with the World Meteorological Organization (WMO) to provide information about categories of users, types of data downloaded, and user locations, to help them understand who is using NOAA satellite data to increase the knowledge of who is using weather satellite data worldwide, e.g. NOAA also collects this information for its own use in order to notify users when there are problems with the satellites that might impact the users' ability to use the data, when there are upcoming changes to satellite systems that need to be broadly circulated, and to occasionally request feedback from users for new requirements, that are then provided to engineers who are building future satellites and products. Occasionally NOAA may use the registration information to notify users of upcoming requirements gathering and training opportunities for systems and products that they already use. That collection operates within the NOAA5004 boundary to make more efficient use of IT resources by combining similar functions under one umbrella.

5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records. An additional authority from NOAA-11 is 15 U.S.C. 1512, Powers and duties of Department.

FROM COMMERCE/DEPT-13; Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

There is information sharing of environmental data only, conducted by the system. PII would be shared, only in the case of security or privacy breach, within the bureau, with DOC bureaus, and with other federal agencies.

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is High.

<u>Section 1</u>: 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		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical	

				Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name*	
s. Other general personal data (specify):					

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	X
b. IP Address	X	d. Queries Run	X	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	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		

Other (specify

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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	X	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): To determine qualifications for data access			

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).

Any PII collected on this system is for the purpose of verifying eligibility for system use, as per government regulation, to track IT system access per government IT security rules, or to provide contact information in cases where troubleshooting interference issues or malfunctioning transmitters are needed. No BII is collected. The information applies to any user of the system, which may include federal employees/contractors, members of the public who meet federal eligibility requirements, or foreign nationals who use the GOES Data Collection System (DCS) in the performance of their normal jobs, e.g. to be able to receive environmental satellite data and processed satellite data products available to the public domain. These DCS users access the system through an Application, which allows them access only to perform functions contained within the application.

There is a survey available to users of NOAA weather satellite data (any of the same categories as may register to use the GOES DCS), including those who do not have satellite ground stations. The survey provides information about who is using NOAA satellite data to increase the knowledge of who is using weather satellite data worldwide NOAA also collects this information for its own use in order to notify users when there are problems with the satellites that might impact the users' ability to use the data, when there are upcoming changes to satellite systems that need to be broadly circulated, and to occasionally request feedback from users for new requirements, that are then provided to engineers who are building future satellites and products.

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	X*		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*For security breach

	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.

	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:
X	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): Foreign nationals who use the GOES application.			

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: https://dcs1.noaa.gov> <https://dcs2.noaa.gov> <https://dcs3.noaa.gov> <https://dcs4.noaa.gov> Please click on the Privacy Act Statement link at the bottom of the page of each of these sites. dcs1 and dcs2 are at Wallops. dcs3 and dcs4 are at NSOF (Suitland).	
X	Yes, notice is provided by other means.	Specify how: Notification is provided on the DCS registration form. "In order to use the Argos DCS, you must complete the system agreement." For the survey, the DCS web sites state: **Register* for Direct Readout and Services Notifications** Help us keep you up to date with changes and anomalies! * This is the survey, completion of which allows for receipt of notifications.
	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: Users are not required to fill out the registration form. However, if they do not fill out the form, they will not qualify for accessing the satellite data. Completion of the survey is completely optional.
	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: Individuals may choose not to complete all information on the registration form, but then registration will not be possible. Completion of the registration form implies consent to the uses of the information, which are stated under Specific Responsibilities of Operator. The survey has several uses as described in the Introduction. The banner on the Web page explains the uses. Consent to those uses is implied by completion and submission of the survey.

	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: Individuals may review/update their PII through their accounts; instructions are given as part of the account agreement.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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.
	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. Yes, DCS uses Tripwire log center and ArcSight audit log tools.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _3/24/2019________________ ☐ 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).
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.

Hardware and software firewalls; Intrusion Prevention system; Central event log servers; Configuration management software, local and remote, Incident reporting software to an offsite location. Access to the database or any of the system processes or components is restricted to system administrators. Members of the public who take the DCS survey are prevented from accessing the data base or any of the system processes or components. Administrators are allowed full access to system components, software and database. NOAA operators and managers are allowed access to various system components based on the role assigned to them by administrators within that application. Additionally, all PII data resides in a database that is encrypted by the TDE (Transparent Data Encryption) technology built in to Microsoft SQL Server.

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)*: Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission Commerce/DEPT-13, Investigative and Security Records
	Yes, a SORN has been submitted to the Department for approval.
	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 1404-04, GOES Data

	Collection System, GOES DCS SUAs.
	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	
Other (specify):			

<u>Section 11</u>: 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.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: There is very little PII.
X	Data Field Sensitivity	Provide explanation: There is no sensitive PII.
	Context of Use	Provide explanation:

	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

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

	Yes, the conduct of this PIA results in required business process changes. Explanation: Increase in privacy controls.
X	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.