Template Version Number: 01-2020

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
Data Collection System

Reviewed by: _____, 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

GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2022.01.06 14:48:22 -05'00'

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 National Environmental Satellite Data and Information Service (NESDIS) operates the Geostationary Operational Environmental Satellites (GOES) and the Polar Operational Environmental Satellites (POES) that are designed to monitor and report the Nation's weather data. In addition to observing that weather from space, both of these series of satellites provide relay services that allow observing systems on the ground to send collected data through the satellites to provide near real time delivery. The relay system that uses GOES is called the GOES Data Collection System (DCS) and the relay system that uses POES is called the Argos Data Collection System. NOAA5004 is the IT system that manages and processes data from the GOES Data Collection System (DCS). GOES DCS is used for monitoring environmental events that may endanger life and property in the U.S., and in neighboring regions, and has therefore been classified as a national critical system.

(a) Whether it is a general support system, major application, or other type of system

NOAA5004 DCS is a Major Application

(a) System location

The ground system and the IT system are operated from the Wallops Command and Data Acquisition Station (WCDAS) Wallops Island, VA and the NOAA Satellite Operations Facility (NSOF) Suitland, MD.

(b) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

DCS interconnects with the following NOAA information system:

- NOAA0550, NOAA Enterprise Network (N-Wave)
- NOAA0100, NOAA Cyber Security Center (NCSC)
- NOAA5045, NOAA Environmental Satellite Processing Center (ESPC)

(a) The way the system operates to achieve the purpose(s) identified in Section 4

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. NOAA requests contact information on that form, 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.

(b) How information in the system is retrieved by the user

Through the DCS Administration and Data Distribution System (DADDS), NOAA's system for managing and providing access to data from GOES DCS, via four publically accessible web servers.
External Users of DCS data include various Federal, state, local and international government agencies, organizations and individuals, such as the NWS, the USGS, the Department of the Interior, Federal Aviation Administration, local flood management programs, etc.

System Access

This is a restricted public access system. All users must have an account and authenticate themselves to DCS. Authorized users have access restricted to only their own files containing demographic

data about themselves and their own Data Collection Platforms (DCP)/Sensors. Public access is allowed to the secure Web Site, but this does not allow direct connection to DCS. The DCS web application allows DCS users and managers selective access to view or modify individual fields and records in the database according to access privileges established by Government DCS Personnel. Access to any database function is based upon the DCS User identification established and verified at the time of the user's logging onto the system.

Each type of table and function shall have defined rules and roles defined by user type and enforced by the web application. Access to the DBMS tables is selectively controlled such that owners/users may view their own file records and modify allowed fields, but have no access to the data of others. If users want to modify their records or access portions of the system, an active login and password must be in the system. Authorized system administrators manage the access level and authorization of users.

External User account management is handled through the database. Users request an account through an online form. The DCS manager authorizes the account after verification. The DCS manager and DCS Technicians manage user account creation and maintenance for the LRGS.

The access level and each user type is outlined below:

Internal DCS User accounts (system administrators, managers and technicians) are managed through Active Directory within the DCS domain. A Domain account request form is required prior to creation of the User account in the DCS domain.

- Level 6: Administrators - Administrators are at the highest level of the DCS web application user hierarchy. DCS administrators have the ability to create, delete, update and view any DCS user of any role, including other administrators. In addition, administrators will have the same privileges for every type of DCS data in the system.
- Level 5: Managers - Managers are at the next highest level of the user hierarchy. They are responsible for maintaining the DCS system and performing tasks such as PDT and CDT management. They have create, delete, update and view privileges for all user roles, except that of administrators. Like administrators, they will have access privileges for all DCS data.
- Level 4: Master Operator - Master operators have the ability to create, delete, update and view both master and standard DCS operators. They do not have the ability to perform these same tasks on any other user type. Master operators consist of the DCS manager at WCDAS and DCS shift leaders.
- Level 3: Standard Operators - Standard operators only have view privileges within the system. Operators should have no need to update any DCS data, like UDTs and PDTs. Standard operators consist of operators below that of master operators at WCDAS.
- Level 2: DCS Master User (Program Administrator) - Master users are the DCS program administrators for organizations. These users have obtained the required SUA/MOA agreement. They have the ability to create, update view and delete standard DCS users. They also have the ability to update most DCS data pertaining to their organization.
- Level 1: DCS Standard User - Standard users are the lowest level in the web application user hierarchy. They cannot create or delete any type of user or data. They have the ability to view

data from their organization only. They also have the ability to update a limited number of UDT and PDT fields

- Level 0: Guests - Guests can only view the login page and submit an SUA request. They have virtually no privileges within the system.

(c) How information is transmitted to and from the system

Information is transmitted to the system through GOES and POES relay services that allow observing systems (sensors) on the ground to send collected data through the satellites via radio frequency (RF) to provide near real time data delivery. The DCS utilizes the latest virtualization techniques where applicable, in addition to reliable and redundant system to provide users with account managed internet access to processed environmental satellite data.

(d) Any information sharing conducted by the system

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, DOC bureaus, and with other federal agencies. A limited subset of information (names, telephone numbers, and email addresses) is shared with Management.

(e) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

• 15 USC 1512 (Powers and Duties of the Department of Commerce) 5 USC 2101 to 10210 (Government Organizations and Employees, Part III, Employees) 5 USC 301 (Departmental Regulations)

• 10 USC 8010 to 9448 (Armed Forces Air Force - Organization, Personnel, and Training)

• 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210 110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

• E.O. 9397; E.O. 12931; 40 U.S.C. Sec. 501- 5 02.

• 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended Version Number: 01-2015 3 by 13478, 9830, and 12107.

• 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107- 347, Sec. 203), as amended by the Federal Information Security Modernization Act of20l4 (Pub. L. 113-283); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork Elimination Act (Pub. L. 105 277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD- 12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

• Sections 1104, 3321, 4305, and 5405 of Title 5, U.S. Code, and Executive Order 12107.

• Federal Acquisition Regulation (FAR) Subparts 4.1 l and 52.204 and 2 CFR, Subtitle A, ChapterI, and Part 25, as well as 40 U.S.C. 12l(c); FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989)

• E-Government Act of 2002 (Pub. L. 107- 347) Section 204; Davis-Bacon and Related Acts: 40 U.S.C. 3141 - 3148 40 U.S.C. 276a; 29 CFR parts I, 3, 5, 6 and 7; Section 5 of the DigitalAccountability and Transparency Act (DATA Act), Public Law 113 - IO1.

• 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.

• Office of Management and Budget Circular A-130, Managing Information as a StrategicResource (July 28, 2016).

• Privacy Act, 5 U.S.C. § 552a. System of Records Notice (SORN), Commerce/NOAA-11, Contact Information for Members of the Public Requesting orProviding Information Related to NOAA's Mission, Commerce/DEPT-13, Investigative and Security Records.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The FIPS 199 classification for NOAA5004 DCS is 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):					

____ This is an existing information system in which changes do not create new privacy

risks, and there is not a SAOP approved Privacy Impact Assessment.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

X This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

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

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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	f. 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 Describe how the accuracy of the information in the system is ensured.

Accuracy of the NOAA5004 information outlined in this assessment and maintained in the system, is ensured during the voluntary online system user agreement form information collection, which is then used to setup and provide access to data products, to distribute notices and updates to authorized DCS users. The system accuracy is further ensured through the implementation of the latest revision of NIST 800-53 security controls as outlined in the system security plan to provide confidentiality, integrity and availability of the information.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648-0157 and 0648-0227
	No, the information is not covered by the Paperwork Reduction Act.

2.5 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			
For a Computer Matching Program		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):			

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.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The internal or insider threat still constitutes a major potential threat to any organization's information system. A robust NOAA employee training program, implementation of NIST 800-53 security controls, annual assessments, annual pen-tests and continuous monitoring of the system mitigates the likelihood an insider would act on the system. NOAA5004 follows all NIST Media Protection (MP) security controls, to include the training, handling, retention and purging of information guidance and NOAA/NESDIS/OSPO requirements.

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

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

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.

X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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.

6.4 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):			

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. Explanation: No BII is collected and the minimal and low level PII that is collected, will not be shared. Access is monitored, tracked and recorded through the federally mandated implementation of the latest revision of NIST 800-53 management, technical and operational security controls as outlined in the system security plan to provide confidentiality, integrity and availability of the information, which is continuous monitored and assessed annually. An example of management controls implemented to monitor, track and record access are through the both the User application process and this required and documented annual PIA/PTA review process.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 03/24/2021 ☐ 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 controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).

X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
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 DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

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 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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, number, and link. *(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 on (date).
	No, this system is not a system of records and a SORN is not applicable.

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 Support User Agreements (SUA).
	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):			

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

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. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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 level. *(Check all that apply.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: There is a minimal amount of 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 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

NOAA5004 system intentionally collects directly from the applicant/user the lowest level andamount of privacy data needed to setup and maintain account and data access for the DCS user community.

12.2 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: The increase of privacy control implementations is ongoing.
	No, the conduct of this PIA does not result in any required business process changes.

12.3 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.

Points of Contact and Signatures

Information System Security Officer or System Owner
Name:Melvin Conser
Office:OSPO
Phone: 757-824-7327
Email:Melvin.G.Conser@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: CONSER.MELVIN.GENE.1507017068 Digitally signed by CONSER.MELVIN.GENE.1507017068 Date: 2021.10.28 15:25:55 -04'00'

Date signed: 10/28/2021

Information Technology Security Officer

Name:Rick Miner
Office:ACIO-S
Phone:301-427-8822
Email:Rick.Miner@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Digitally signed by MINER.RICHARD.SCOTT.1398604519 Date: 2021.11.12 09:10:27 -05'00'

Date signed:

Privacy Act Officer
Name:Adrienne Thomas
Office:NOAA OCIO
Phone:240-577-2372
Email:Adrienne.Thomas@noaa.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2022.01.06 08:42:07 -06'00'

Date signed:

Authorizing Official
Name:Mark S. Paese
Office:NESDIS
Phone:301-713-2010
Email:mark.paese@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: PAESE.MARK.STEFAN.1365833202 Digitally signed by PAESE.MARK.STEFAN.1365833202 Date: 2022.01.06 08:00:34 -05'00'

Date signed:

Bureau Chief Privacy Officer
Name:Mark Graff
Office:NOAA OCIO
Phone:301-628-5658
Email:Mark.Graff@noaa.gov

I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.

Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.01.06 14:06:20 -05'00'

Date signed: 14447892

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.