U.S. Department of Commerce
NOAA

**Privacy Threshold Analysis
for the
Data Collection Systems
(DCS)
NOAA5004**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA DCS

Unique Project Identifier: NOAA5004

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 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

b) *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.

c) *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)

d) *The purpose that the system is designed to serve*

The purpose of the DCS is to collect data from the government sponsored and government-owned Data Collection Platforms (DCP) and disseminate the data to all users of the DCS service. The data consists of but is not limited to measurement observations of wind speed, wave height, water depth, temperature, etc. 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.

e) *The way the system operates to achieve the purpose*

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 DCP data via the Local Readout Ground Stations (LRGS). 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.

f) *A general description of the type of information collected, maintained, use, or disseminated by the system*

There is environmental data and both user and administrator/technician account information a collected, maintained and disseminated by the system. No BII is collected. The minimal amount of collected PII is not shared, however, only in the case of security or privacy breach, the limited subset of information (names, telephone numbers, and email addresses) is shared internally with Management and may be shared within the bureau, DOC bureaus and or with other federal agencies. The data/account information for the Administrators/Technicians who manage User account creation and maintenance of the DCS system is the same information NOAA requires during the hiring process and to setup and maintain administrative NOAA email and domain accounts and, is not disseminated outside of the DCS boundary, except in

case of a security or privacy breach as outlined above.

g) Identify individuals who have access to information on the system

There are two distinct types or groups who access information on the system. The first are the external 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, through the four public DCS websites only. These external members/users do not have access to any of the internal DCS devices/systems. The second group consists of system administrators, managers and technicians who maintain, secure and operate the system and who are vetted by the NOAA/government hiring/onboarding process and are further monitored, tracked and recorded per federally mandated regulations and implemented system security controls.

h) 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 anyrole, including other administrators. In addition, administrators will have the same privileges for everytype 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 havecreate, 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 anyother 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. Theyhave 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.

i) 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

    _____   This is a new information system. *Continue to answer questions and complete certification.*

    _____   This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

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. *Continue to answer questions and complete certification.*

    _____   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). *Continue to answer questions and complete certification.*

    _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). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

    _____   Yes. This is a new information system.

    _____   Yes. This is an existing information system for which an amended contract is needed.

    _____   No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

    _X_   No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

    NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

    _____   Yes. *(Check all that apply.)*

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

     X   No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

    As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

    _____   Yes, the IT system collects, maintains, or disseminates BII.

     X   No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)
4a. Does the IT system collect, maintain, or disseminate PII?

    As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

     X   Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

         X   DOC employees
         X   Contractors working on behalf of DOC
        _____   Other Federal Government personnel
         X   Members of the public

        _____   No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

       Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

  X   No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

  X   Yes, the IT system collects, maintains, or disseminates PII other than user ID.

       No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

       Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

  X   No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

 X   I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____   I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner	**Information Technology Security Officer**
Name:Melvin Conser Office:OSPO Phone:757-824-7327 Email: Signature: CONSER.MELVIN.GENE.1507017068 _Digitally signed by CONSER.MELVIN.GENE.1507017068 Date: 2021.10.28 15:27:58 -04'00'_ Date signed: 10/28/2021	Name:Rick Miner Office:ACIO-S Phone:301-427-8822 Email:Rick.Miner@noaa.gov Signature: _Digitally signed by MINER.RICHARD.SCOTT.1398604519 Date: 2021.11.12 09:05:48 -05'00'_ Date signed:
Privacy Act Officer	**Authorizing Official**
Name:Adrienne Thomas Office:NOAA OCIO Phone:240-577-2372 Email:Adrienne.Thomas@noaa.gov Signature: THOMAS.ADRIENNE.M.1365859600 _Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2022.01.06 08:43:52 -06'00'_ Date signed:	Name:Mark S. Paese Office:NESDIS Phone:301-713-2010 Email:mark.paese@noaa.gov Signature: PAESE.MARK.STEFAN.1365833202 _Digitally signed by PAESE.MARK.STEFAN.1365833202 Date: 2022.01.06 08:00:03 -05'00'_ Date signed:
Bureau Chief Privacy Officer	
Name:Mark Graff Office:NOAA OCIO Phone:301-628-5658 Email:Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 _Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.01.06 13:52:46 -05'00'_ Date signed:	