Privacy Threshold Analysis
for the
NOAA5004 (Data Collection System – DCS)
U.S. Department of Commerce Privacy Threshold Analysis

NOAA5004 DCS System

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 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.
Questionnaire:

1. 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.*

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>g. New Interagency Uses</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</td>
</tr>
</tbody>
</table>

   ___ 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 later). *Skip questions and complete certification.*

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. *Please describe the activities which may raise privacy concerns.*

   ___ 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.553(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 about: (Check all that apply.)

___ Companies
___ Other business entities

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

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

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
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 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.

4c. 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, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.
CERTIFICATION

☑️ I certify the criteria implied by one or more of the questions above apply to the DCS LAN, NOAA5004 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 DCS LAN, NOAA5004 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):
Johnny R. Clark

Signature of ISSO or SO: CLARK.JOHNNY.R.1365842791 Digitally signed by CLARK.JOHNNY.R.1365842791 Date: 2019.09.13 14:06:29 -04'00'  Date: 8/13/19

Name of Information Technology Security Officer (ITSO): Frank Menzer

Signature of ITSO: MENZER.FRAN.K.E.1026670450 Digitally signed by MENZER.FRAN.K.E.1026670450 Date: 2019.09.13 18:23:48 -04'00'  Date: 8/19/19

Name of Authorizing Official (AO): Mark S. Paese

Signature of AO: Mark S. Paese  Date: 8/22/19

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514.447892 Digitally signed by GRAFF.MARK.HYRUM.1514.447892 Date: 2019.09.13 15:41:34 -04'00'