U.S. Department of Commerce (DOC)
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)

Privacy Threshold Analysis (PTA)
For the
Wallops Command and Data Acquisition Station Administrative Local Area Network (NOAA5032)

Version: 1.0
February 12, 2018

U.S. Department of Commerce Privacy Threshold Analysis

Office of Satellite and Product and Operations (OSPO)

Unique Project Identifier: NOAA5032

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:
(a) The Wallops Command and Data Acquisition Station (WCDAS) Administrative LAN (NOAA5032) is a General Support, office automation system that (b) is located within the WCDAS computer facility in Wallops Island, VA. (c) NOAA5032 relies on the NOAA NOC (NOAA 0200) for e-mail, and VPN access to NSOF (NOAA5044) for Internet connectivity. (d) The WCDAS Administrative LAN supports the NESDIS mission by providing IT resources to WCDAS personnel. Specifically, it is used to support electronic mail, purchasing, logistics, facility management, inventory, human resource, contract administration, general management functions and office automation functions (e) The WCDAS Administration LAN enables communication among OSPO and various NOAA groups to conduct administrative functions which include daily, weekly, monthly, and annual reports. The WCDAS Administration LAN is used to support electronic mail (GMAIL) through the use of Google, purchasing, logistics, facility management, inventory, human resource, contracts administration, general management functions, and office automation functions. (f) Types of data transiting thru or residing on the WCDAS Administration LAN include administrative email messages, data concerning time and attendance reports, status reports, travel orders, Federal grants, environmental monitoring, budget and capital planning, contingency planning, facilities management, workplace policy, human resources, goods acquisition, and IT infrastructure management. Data transiting or resident on the WCDAS Administrative LAN are typically in the form of e-mail messages, Excel spreadsheets, word processing documents, CAD drawings and simple databases resident on individual workstations. (g) The Users community of the WCDAS Administration LAN include management, technical, operations and administrative staff located at the Wallops Command and Data Acquisition Station. (h) Workstations located in the users' offices are used by the operational personnel, to log into their own user accounts on the WCDAS Domain where they can perform various administrative functions, and print to local and / or network printers. (i) A

dedicated DS-3 link provides the Wide Area Network (WAN) access from WCDAS Administration LAN to and from the Internet through the NOAA NOC.

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).

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.*

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.*

_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 01-2015 or later). *Continue to answer 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.*

__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 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
____ Contractors working on behalf of DOC
____ 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

__X_ I certify the criteria implied by one or more of the questions above **apply** to the Wallops Command and Data Acquisition Station Administrative Local Area Network 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 Wallops Command and Data Acquisition Station Administrative Local Area Network and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Owner (SO): Johnny R. Clark

Signature of SO: CLARK.JOHNNY.R.1365842791 Digitally signed by CLARK.JOHNNY.R.1365842791 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=CLARK.JOHNNY.R.1365842791 Date: 2018.02.14 09:32:40 -05'00' Date: 2/14/2018

Name of Information Technology Security Officer (ITSO): Nancy A. DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.02.14 15:01:31 -05'00' Date: 02/14/2018

Name of Authorizing Official (AO): Vanessa L. Griffin

Signature of AO: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.01 14:40:34 -05'00' Date: _____

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

Signature of BCPO: _____ Date: _____