Version Number: 01-2015

U.S. Department of Commerce
[Bureau Name]

Privacy Threshold Analysis
for
NOAA6101

U.S. Department of Commerce Privacy Threshold Analysis

NOAA6101

Unique Project Identifier: [Number]

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:

System NOAA6101 is a general support system used to ensure that the Office for Coastal Management's (OCM's) scientific and internal administrative I operational needs are met. The system is an integrated collection of subsystems designed to provide general office automation, infrastructure, and connectivity services to the National Oceanic and Atmospheric Administration's (NOAA) Office for Coastal Management (OCM) located in Charleston, SC, Silver Spring, MD, Honolulu, HI, Stennis Space Center, MS, additional OCM field offices, and remote staff The system enables OCM to achieve its mission, which is to support the environmental, social, and economic well-being of the coast by linking people, information, and technology. OCM assists the nation's coastal resource Management community by providing access to information, technology, and training, and by producing new tools and approaches that often can be applied nationwide.

Two of the component subsystems are the file servers and Web Application Subsystem (WAS). While the file servers store and serve up administrative and operational data, the WAS hosts and serves data-driven Web-based applications. Applications served from an internal Web server are accessible only to NOAA employees and contractors operating from within the NOAA network. These internal applications track information related to OCM's operations I administration. Applications served from public-facing Web servers may be intended for OCM and other subsets of OCM, NOAA, other federal agencies, customers, partners, and/or the public.

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):					

__x__ This is an existing information system in which changes do not create new privacy risks. *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.

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

Activities are focused on internal administrative efforts (employee information), web-based inquiries and information sharing, and business specific information (contracts, proposals, etc…). All are protected in ways detailed in the Privacy Impact Assessment (PIA) for NOAA 6101.

____ 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.)."

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

___x_ Companies
__x__ Other business entities

____ 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

_x___ I certify the criteria implied by one or more of the questions above **apply** to the NOS Office for Coastal Management (OCM) 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.

Name of Information System Security Officer (ISSO) or System Owner (SO): Chuck Baxley (ISSO)

Signature of ISSO or SO: BAXLEY.CHARLES.A.III.1058676264 Digitally signed by BAXLEY.CHARLES.A.III.1058676264 Date: 2018.01.10 11:08:07 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker (ITSO)

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.01.24 08:14:31 -05'00' Date: _____

Name of Authorizing Official (AO): Jeffrey L. Payne (AO)

Signature of AO: PAYNE.JEFFREY.L.DR.1365833881 Digitally signed by PAYNE.JEFFREY.L.DR.1365833881 Date: 2018.01.10 17:55:59 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____MARK GRAFF_____

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.25 17:12:54 -05'00' Date: _____