U.S. Department of Commerce
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the
Pacific Islands Region Office (PIRO)
U.S. Department of Commerce Privacy Threshold Analysis
National Oceanic and Atmospheric Administration
/ Pacific Islands Region Office

Unique Project Identifier: 006-48-01-14-02-3305-00

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 NOAA Fisheries Pacific Islands Regional Office (PIRO) Local Area Network (LAN) functions as the overall General Support System (GSS) for PIRO located in Honolulu, Hawaii. Additional remote sites exist in Samoa, Guam and Saipan. The information system provides administrative support typically found in administrative offices within the federal government as well as supplemental operational services.

PIRO consists of the following divisional units:

• PIR Regional Administrators Office
• NOAA Office of General Counsel
• PIR Habitat Conservation Division
• PIR International Fisheries Division
• PIR Observer Program
• PIR Office of Management and Information
• PIR Protected Resources Division
• PIR Sustainable Fisheries Division

The categories of data collected, stored and disseminated include administrative, human resources, operations, statistical, economic, and technical.

NOAA4920 is located at the following locations: Honolulu, HI, American Samoa, the Commonwealth of the Northern Mariana Islands, and Guam. The primary functions of the NOAA4920 information system are:

• File and printer sharing
• Web applications and database services
• Access to NOAA/DOC web services via wide area network connections
• Pacific region fisheries permit data repository

No major application systems exist within NOAA4920.

**Questionnaire:**

1. What is the status of this information system?

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

   _X_ 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>d. Significant Merging</td>
</tr>
<tr>
<td>e. New Public Access</td>
</tr>
<tr>
<td>f. Commercial Sources</td>
</tr>
<tr>
<td>g. New Interagency Uses</td>
</tr>
<tr>
<td>h. Internal Flow or Collection</td>
</tr>
<tr>
<td>i. Alteration in Character of Data</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</td>
</tr>
<tr>
<td>Use of E-Discovery software to comply with Freedom of Information Act (FOIA) requests</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). *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.).”

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

__X__ Companies

___  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 NOAA4920 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): __Nicholas J. Tenney__________________________

Signature of ISSO or SO: TENNEY.NICHOLAS.JAMES 1407926966

Digitally signed by TENNEY.NICHOLAS.JAMES.1407926966
Date: 2018.04.20 08:23:17 -10'00'

Date: ___4/11/18___

Name of Information Technology Security Officer (ITSO): __Catherine Amores__________________________

Signature of ITSO: AMORES.CATHERINE.OLLEDAD.1541314390

Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390
Date: 2018.04.23 13:21:54 -04'00'

Name of Authorizing Official (AO): __Michael Tosatto__________________________

Signature of AO: TOSATTO.MICHAEL.D.101

Digitally signed by TOSATTO.MICHAEL.D.101 4020922
Date: 2018.04.20 14:49:41 -10'00'

Name of Bureau Chief Privacy Officer (BCPO): __Mark Graff__________________________

Signature of BCPO: GRAFF.MARK.HYRUM.151444

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: 2018.04.23 16:04:04 -04'00'