Privacy Threshold Analysis
for the
NOAA6101 - NOS Office for Coastal Management (OCM) General Support System
U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOAA6101 - NOS Office for Coastal Management (OCM) General Support System

Unique Project Identifier: 006-48-02-00-01-0511-00

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:

a) Whether it is a general support system, major application, or other type of system

NOAA6101 is a general support system used to ensure that the Office for Coastal Management’s (OCM’s) programmatic and internal administrative 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).

b) System location

FLETC, North Charleston, SC
IRC, Honolulu, HI
Stennis Space Center, MS
Ronald V. Dellums Federal Building, Oakland, CA
Silver Spring Metro Center (SSMC), Silver Spring, MD
Microsoft Azure - US East 2, US Central

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

This is a standalone system

d) The purpose that the system is designed to serve

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. The OCM Strategic Plan addresses three strategic outcomes for the coastal management community: healthy coastal ecosystems, resilient coastal communities, and vibrant and sustainable coastal economies.

\( e \) The way the system operates to achieve the purpose

NOAA6101 groups elements of the system into three areas, each of which serves a distinct and specific function:

- Network Devices – NOS/OCM Wide Area Network (WAN) and OCM wide area network.
- NOS Domain Servers -- The NOS domain infrastructure components and OCM Local Area Network (File, Print, Application) services.
- Web Application Servers -- OCM application and database hosting services

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

PII is collected to communicate with OCM customers and stakeholders on topics where they have an explicitly expressed professional interest, or have made a specific request for data or information.

Other PII is collected for OCM staff employment and personnel records (federal/contractor) and OCM visitor access information (federal/contractor/member of the public/foreign national).

BII is collected and maintained for purposes such as contractual agreements and grants.

Details are found below.

NOAA’s Office for Coastal Management Business Operations Division collects data containing personally identifiable and business identifiable information (BII) for internal government operations / administrative processes. The processes include:

- Employee / Contractor information needed for personnel, performance evaluation, merit rewards, training, travel, accident reporting, etc. This type of PII information is reviewed and updated annually by staff.
- Employee / Contractor / Visitors / Foreign National information required by DOC and/or OPM for security purposes and/or background checks. Passport numbers are collected for foreign visitors, sent as appropriate for security checks, and removed from the system. All information is required per DOC PII Policy and Foreign National Processing guidance, as well as the Federal Law Enforcement Training Center (FLETC) Foreign National Visitor Process.
- Employee / Contractor emergency contact information for use in call trees and Continuity of Operations Plan (CoOP), which includes names, phone numbers, and addresses
- Applicant information submitted in response to requests for proposals and/or in response to a
solicitation. External grant applications/proposals are not typically collected by OCM. Per the NOAA Grants Management Office policy, proposals almost always run through the Grants.gov submission process and end up in the Grants Online system. In rare cases, applicants without access to the Internet [e.g., US Territories] are permitted to submit paper applications. When this happens, OCM scans the proposals and loads them into Grants Online. Any subsequent sharing of grant proposals via email for review must be done via a secure file transfer process (e.g., Grants Online, Accellion/Kiteworks if emailing internally or externally to NOAA, a secure Google Drive or a network location for internal NOAA reviewers, or a password protected website for internal and external NOAA reviewers). Once reviews are complete and awards are made, proposals are removed from the OCM system and the Grants Online system is the official repository.

Typical personal or business identifiable information collected for grant applications includes:

- proposer's name
- email
- phone 
- organization name
- organization DUNS 
- employer identification number or taxpayer identification number

For acquisitions, the business identifiable information collected typically includes:

- proposer's name
- email
- phone 
- organization name
- organization DUNS 
- Cost proposal information is also collected, and would be considered BII, as it is often proprietary.
- Management and technical approaches found in vendor proposals is often considered BII.

Other PII that is being collected and/or made available via Internet / Web sites or applications include the following.
(Any personal information on any of the following sites is entirely voluntary and can be removed by request at any time.)

- PRiMO: Web site that publicly lists some partner organization POCs (name, organization, email, phone number, photos), along with OCM POCs, leadership names and photos, Conference Programs with varying number of presenters information. POC information is entirely voluntary and can be removed at any time upon request. All of PRiMO’s past conference programs are available as pdf documents with session presenters listed with their abstracts.
- OCM Intranet (Inet): Contains current information on staff, including phone numbers, names, email addresses, and emergency contacts. The system is used to maintain up to date records on staff contact information.

- Task Order Management Information System (TOMIS): Version 2 (V2) is currently under development with a release date in July 2020. Version 1 (V1) will be no longer accessible when V2 is released.
  - V2: Application that collects and maintains POC information (name, email, phone, company name) for use in administering various contractor tasks and deliverables. Note, contractor evaluations will not be migrated to the new site or database.
  - V1: Application that collects and maintains POC information (name, email, phone, company name, contractor evaluations) for use in administering various contractor tasks and deliverables. After migration to V2, the V1 DB will be backed up, encrypted and taken offline. Contractor evaluations will be deleted and will not be backed up as part of the database archiving process.

- National Estuarine Research Reserves (NERRS): Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.

- Estuaries Education: Web site that publicly lists some partner organization POCs (name, organization, email, phone number), along with OCM POCs. POC information is entirely voluntary and can be removed at any time upon request.

- Digital Coast: Publishes contact information of trainers for some trainings listed on the Digital Coast Training page. Information includes name, email, and location. Permission is acquired (via a form) from each trainer before listing their information on the site.

- Ocean Law Search: Web site related to underwater cultural heritage that makes various public laws, statutes, articles, and court case summaries available via an online searchable interface. All of the information available is publicly accessible and has been assembled to focus on underwater cultural heritage. Some of the documents available contain names and addresses of legislators, attorneys, plaintiffs, or witnesses.

- CAMMP: Version 2 (V2) is currently under development with a release date in August 2020. Version 1 (V1) will be no longer accessible when V2 is released.
  - V2: Application that allows for collaborative project planning with partners (state CZM and NERRS). Data collected includes names, title, email, and budget.
  - V1: Application that allows for collaborative project planning with partners (state CZM and NERRS). Data collected includes names, title, email, and budget.

- Coral Database: Application that collects internal NOAA staff proposals to the NOAA Corals matrix program.

- Data Access Viewer (DAV): Application that receives requests for data from the public. Email addresses are stored to provide a method of contacting the requester when the data is ready for pickup on the OCM FTP site.

- Training Manager System: Web site that collects information on training courses, hosts, and participants of OCM training programs. Information that is collected is not shared publicly. Fields
collected include (name, organization, address, city, state, zip, email, phone).

- **OCM Point of Contact Management Database:** Centralized contact management database used to maintain information from customers who have requested data or information, participated in conferences, requested products/materials, or attended meetings or trainings offered by OCM. This is a secure and centralized database. Fields collected include (name, title, organization, address, city, state, zip, country, email, phone).

- **NERRs and State Coastal Zone Management (CZM) Performance Measures Databases** are authenticated applications for NERRs and CZM partners to document grant performance measures in a standardized way, and to work collaboratively with OCM staff. Information collected includes name, organization, email, and phone number.

- **Coastal Zone Management Act Program Changes** is an application where proposed State CZM Program changes are posted for public comment. Information collected includes name, affiliation, email address, city, state, zip, comments. Email address is collected to verify user exists and a two step authentication process is in place to make sure the user receives an email before comments are posted.

- **Green Infrastructure Database** is a catalog of literature resources documenting the effectiveness of using green infrastructure to reduce impacts from coastal hazards. Information published includes study authors as typical with standard citations.

- **OCM Staff Info - Contact information for OCM staff.** Information published includes name, email and phone number.

- **Coral Reef Task Force - Website used for publishing documents, policies, reports, and presentations from the Coral Reef Task Force meetings.** Information published includes presenter names and organizations.

- **Virtual Conferencing and Webinars - Adobe Connect is being used for virtual meetings and webinars.** Adobe Connect is being used for virtual meetings and webinars. Recorded webinars are stored on Adobe site. Attendee information is anonymized when saved for republishing.

- **Still images and video on web sites, online newsletters, video streaming, to fulfill OCM’s mission to provide coastal information to interested stakeholders and the general-public.**

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

The users of the NOAA6101 systems that collect non-sensitive PII and BII are authorized government and contractor workers within the program office and select partners. These systems are not accessible to the public. Public access of information is provided by web application interfaces.

**h) How information in the system is retrieved by the user**

The information is retrieved through an application user interface, except for the data that is kept on the shared drives. Public access of information is provided by web application interfaces.
i) How information is transmitted to and from the system.

PII is manually entered into the system by the administrator or through a bulk upload from a spreadsheet(s).

Social Security numbers are collected for new NOAA/NOS/OCM employees. These are transmitted to the NOAA Security Office via secure electronic transmission and then destroyed. OCM does not maintain them on the IT system or as hard copy files. Passport numbers are handled in the same way as SSNs. Taxpayer or employer ID information is collected infrequently, but is stored only temporarily on the system.

POC information is entered into various applications/web sites as detailed in Section 5 below. This POC information generally consists of name, email, phone number, organization name, and is collected for the following reasons (not exhaustive, and not applicable to each application/site - see Section 5 for specific details):

- preparing collaborative partner project plans
- requesting delivery of data or information
- posting of subject matter expert contact information
- requesting training
- managing task order information
- joining webinars

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>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>
</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). 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 01-2017 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.

X Yes. (Check all that apply.)

<table>
<thead>
<tr>
<th>Activities</th>
<th></th>
<th>Activities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio recordings</td>
<td>x</td>
<td>Building entry readers</td>
<td>x</td>
</tr>
<tr>
<td>Video surveillance</td>
<td>x</td>
<td>Electronic purchase transactions</td>
<td></td>
</tr>
<tr>
<td>Other (specify):</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio recordings: Virtual Conferencing and Webinars - Adobe Connect is being used for virtual meetings and webinars. Recorded webinars are stored on Adobe site, and when appropriate (i.e. trainings and webinars) published for later viewing.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video Surveillance: Video monitoring occurs in the Charleston, SC office at the front door. The video is streamed to an individual's desk for monitoring, but the data is not recorded, saved, or stored.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Building Entry Readers: Information is captured for physical access to OCM buildings.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

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
   ___ National Institute of Standards and Technology Associates
   X  Contractors working on behalf of DOC
   X  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?

   X  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.
   Employee / Contractor / Visitors / Foreign National information required by DOC and/or OPM for security purposes and/or background checks. Passport numbers are collected for foreign visitors, sent as appropriate for security checks, and removed from the system. All information is required per DOC PII Policy andForeign National Processing guidance, as well as the Federal Law Enforcement Training Center (FLETC) Foreign National Visitor Process. All forms and correspondence is encrypted between FLETC and NOAA6101.

   Provide the legal authority which permits the collection of SSNs, including truncated form.
   5 U.S. Code § 552a
   DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
   OPM/GOVT-1, General Personnel Records

   ___ 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.

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 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 NOS Office for Coastal Management (OCM) 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

Signature of ISSO or SO:

BAXLEY.CHARLES.A.III.1058676264 Digitally signed by BAXLEY.CHARLES.A.III.1058676264
Date: 2020.07.30 11:09:14 D:41 a-t04'00'

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

Signature of ITSO:

PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914
Date: 2020.08.03 07:19:54 D:4-04'00'

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO:

THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600
Date: 2020.08.03 09:52:14 D:4-04'00'

Name of Authorizing Official (AO): Jeff Payne

Signature of AO:

PAYNE.JEFFREY.L.DR.1365833881 Digitally signed by PAYNE.JEFFREY.L.DR.1365833881
Date: 2020.07.30 14:24:21 D:4-04'00'

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

Signature of BCPO:

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2020.08.03 11:03:26 D:4-04'00'