

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



**Privacy Threshold Analysis for the
NOAA1200**

Corporate Services / CorpSrv

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/CIO/Corporate Services

Unique Project Identifier: NOAA1200

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: *Provide a brief description of the information system.*

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).

NOAA1200/CorpSrv is a General Support System (GSS) supporting approximately 2,721 end users and consisting of multiple types of subsystems. NOAA1200 administers approximately 3346 workstations/servers at ten sites across the United States, and approximately 2,500 mobile devices (including smart phones, iPads, etc.). For workstations and servers, all sites are bound under an active directory domain structure (CorpSrv.NOAA.local). Windows based devices include domain controllers (DC), file and print servers, desktop / laptop workstations. NOAA1200 supports NOAA’s Line offices (NWS, OAR, OMAO and NESDIS (Coop)), Executive offices and Corporate financial and administrative Program Support Units (PSU).

Address the following elements:

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

NOAA1200 / CorpSrv, is a General Support System (GSS) consisting of multiple subsystems. The NOAA1200 core system consists of user desktop and laptop workstations, Microsoft Windows’ file and print servers, a limited number of network infrastructure components that support NOAA’s executive offices and corporate financial and administrative services Program Support Units located at sites within the United States.

b) System location

1. Silver Spring, MD, (SSMC1 - SSMC4); 2. Washington, DC; 3. Norfolk, VA (two locations); 4. Kansas City, MO, 5. Boulder, CO; 6. Newport, OR; 7. Fairmont, WV, 8. Honolulu, HI, 9. Seattle, WA (two locations), 10. Norman, OK and 11. Frederick, MD.

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

NOAA1200 is hosted in the NOAA network infrastructure and is not a standalone system. NOAA4920 - Pacific Islands Regional Office (PIRO) Network connects to NOAA1200. NOAA0900 – leverages cloud and utilize enterprise services NOAA0700 – Identity, Credential, and Access Management (ICAM), Public Key Infrastructure (PKI services), and Enhanced Security Administration Environment (ESAE). NOAA0550 - N-WAVE for datacom infrastructure between the various headquarters and regional offices.

d) The purpose that the system is designed to serve

The NOAA1200 core system consists of user desktop and laptop workstations, Microsoft Windows' file and print servers, and a limited number of network infrastructure components that support NOAA's executive offices and corporate financial and administrative services.

e) The way the system operates to achieve the purpose

NOAA 1200 supports a user base of approximately 3,000 users and provides connectivity to the NOAA network infrastructure for both local and remote access to the following basic administrative services: collaboration platforms include Google Suite for email and collaboration, network file servers, printing, file backup and restoration, and account management. Residual data from other privacy systems may be stored, and/or processed on user workstations or file servers.

NOAA1200 workstations allows Application Information System (AIS) users (including Trusted Agents) to connect to other (non NOAA1200) privacy systems of record. The process of submitting, retrieving and storing sensitive information varies with each of the various privacy systems users connecting via CorpSrv workstations.

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

NOAA1200 provides connectivity to the NOAA network infrastructure for both local and remote access. VPN is required for network file servers, printing; file backup and restoration; and account management.

Trusted Agents and other users access privacy systems with CorpSrv workstations. Trusted Agents and other users may store Form CD591 (PIV request form) used for government issued identification cards on CorpSrv systems for archival purposes. These records which are submitted and processed in other government privacy systems of record may include fingerprints and a photograph, driver's license and passport numbers. OF-306 Declaration for Federal Employment may be archived in CorpSrv when scanned for submission to a personal security office. Information is collected from federal employees, contractors, and the public who are applying for federal or contractor status.

Information will be accessed only within the bureau, with the case by case exception that information may be disclosed to another Federal agency in connection with the assignment, hiring or retention of an individual, the issuance of a security clearance, the reporting of an investigation of an individual.

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

NOAA1200 users (federal employees and contractors) access data among various hosted applications, including Acquisition and Grants Office, Office of Civil Rights, Office of Human Capital Services, General Counsel and the Office of the Chief Financial Officer, among others. Each organization grants access based on individual and group authorizations and need to know. These access controls are not administered by the IT staff.

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

NOAA1200 users (federal employees and contractors) access data via CorpSrv workstations. Each organization grants access based on individual and group authorizations and need to know. These access controls are not administered by the IT staff.

i) How information is transmitted to and from the system

NOAA1200 provides connectivity to the NOAA network infrastructure for both local and remote access. VPN is required for network file servers, printing; file backup and restoration; and account management. NOAA1200 communications are encrypted in transit via HTTPS, SSH, RDP and VPN connections.

Questionnaire:

1. Status of the Information System

1a. 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): There have been new interconnections with NOAA1200 and location changes.				

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. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

Yes. This is a new information system.

Yes. This is an existing information system for which an amended contract is needed.

No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

No. This is not a new information system.

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. (*Check all that apply.*)

Activities			
Audio recordings		Building entry readers	<input checked="" type="checkbox"/>
Video surveillance		Electronic purchase transactions	
Other (specify):			

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.

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."

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

- DOC employees
- Contractors working on behalf of DOC
- Other Federal Government personnel
- 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.

Social Security numbers are used for government issued identification cards and hiring and retention of employees.

Provide the legal authority which permits the collection of SSNs, including truncated form.

5 U.S.C 1302; 44 U.S.C. 3101; 5 U.S.C. 5379; and Executive Orders 9397, as amended by 13478, 9830, and 12107. SORN COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies

— 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.

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

CERTIFICATION

The criteria implied by one or more of the questions above **apply** to the NOAA1200 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

The criteria implied by the questions above **do not apply** to the NOAA1200 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p>Information System Security Officer or System Owner</p> <p>Name: Bamidele Arawole Office: NOAA OCIO SDD Phone: 202-967-8162 Email: Bamidele.arawole@noaa.gov</p> <p>Signature: Bamidele Date signed: Arawole</p>	<p>System Owner</p> <p>Name: Jason Rickett Office: NOAA OCIO SDD Phone: 240-532-1171 Email: Jason.rickett@noaa.gov</p> <p>RICKETT.JASO Signature: N.ALLEN.1392 Date signed: 392951</p>
<p>Information Technology Security Officer</p> <p>Name: Ansaruddin Hasan Office: NOAA OCIO CSD Phone: 240-255-8556 Email: ansaruddin.hasan@noaa.gov</p> <p>Signature: HASAN.ANSARUDD IN.ISA.1376816210 Date signed</p>	<p>Authorizing Officer</p> <p>Name: Douglas Perry Office: NOAA OCIO Phone: 301-713-7673 Email: Douglas.A.Perry@noaa.gov</p> <p>PERRY.DOUGLAS. Signature: ALLEN.136584727 Date signed: 47270</p>
<p>Privacy Act Officer</p> <p>Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: robin.burress@noaa.gov</p> <p>Signature: Date signed</p>	<p>Co-Authorizing Officer</p> <p>Name: Cameron Shelton Office: NOAA OCIO Phone: 301-628-5721 Email: Cameron.shelton@noaa.gov</p> <p>SHELTON.CA Signature: MERON.LYLE. Date signed: 1365843313</p>
<p>Bureau Chief Privacy Officer</p> <p>Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov</p> <p>Signature: Date signed</p>	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.