Version Number: 01-2020

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/OCIO/Corporate Services

Unique Project Identifier: NOAA1200 / CorpSrv

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: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

Changes from previous year:
Significant change that reduced NOAA1200 privacy risks; all Cloud Service Providers moved to NOAA 0900: Google Apps for Gov't, IBM MaaS360 with Watson, ServiceNOW, AODocs, and Smartsheet.

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. Boulder, CO; 2. Fairmont, WV; 3. Germantown, MD; 4. Honolulu, HI; 5. Kansas City, MO; 6. Newport, OR; 7. Norfolk, VA; 8. Norfolk, VA; 9. Seattle, WA; 10. Silver Spring, MD; 11. Tampa, FL; 12. Washington, DC.

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 not a standalone system.

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

NOAA1200 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 includes 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

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, Workforce Management office, 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

NOAA 1200 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.

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.*

_XX_ 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): Significant change that reduce NOAA1200 privacy risks; all Cloud Service Providers moved to NOAA 0900: Google Apps for Gov't, IBM MaaS360 with Watson, ServiceNOW, AODocs, and Smartsheet.					

____ 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 01-2017). *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 01-2019 or later). *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.

_XX_ 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.

_XX_ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	XX
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.)."

_XX_ 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."

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

_XX_ DOC employees
_XX_ Contractors working on behalf of DOC
_XX_ Other Federal Government personnel
_XX_ 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?

_XX_ 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. 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?

_XX_ 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.

_XX_ 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

I certify the criteria implied by one or more of the questions above **apply** to NOAA1200 / CorpSrv and as a consequence of this applicability, I will perform and document a PIA for this IT system. [CAC/PIV Digital Signatures]

Information System Security Officer Name: Tom Grigsby Office: OCIO SDD Phone: (301) 628-5720 Email: cameron.shelton@noaa.gov	**Information Technology Security Officer** Name: Charles Obenschain Office: NOAA OCIO CSD Phone: (301) 817-3898 Email: charles.obenschain@noaa.gov
GRIGSBY.THOMAS.W.1049202896 Digitally signed by GRIGSBY.THOMAS.W.1049202896 Date: 2021.02.05 22:11:48 -05'00'	OBENSCHAIN.CHARLES.THOMAS.1506347293 Digitally signed by OBENSCHAIN.CHARLES.THOMAS.1506347293 Date: 2021.02.08 07:04:34 -05'00'
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 828-257-3148 Email: Adrienne.Thomas@noaa.gov	**Authorizing Official** Name: Douglas Perry Office: NOAA Deputy OCIO Phone: (301) 713-7673 Email:Douglas.A.Perry@noaa.gov
THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.02.09 13:13:57 -06'00'	PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2021.02.09 09:56:39 -05'00'
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov	
GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.02.24 11:24:05 -05'00'	