Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA0520

NOAA Enterprise Data Centers (EDC)

Version Number: 01-2021

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/OCIO/SDD/Enterprise Data Centers

(EDC)

Unique Project Identifier: NOAA0520

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).

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

The National Oceanic & Atmospheric Administration (NOAA) Enterprise Data Center (EDC) NOAA0520 is comprised of several "subsystems" or "locations." NOAA0520 is a general facility support system. The EDC is responsible for the overall management of operations and oversight at NOAA's Enterprise Data Center locations. The EDC NOAA0520 is missioned with a primary function requirement to provide co-location services which include common controls to the various NOAA programs who reside in the various rooms, buildings, or facilities managed under the EDC umbrella. This information system is also capable of supporting Supervisory Control and Data Acquisition (SCADA) information system (IS) which provides building power, badging and CCTV security support services and resources in select locations.

For the NOAA0520, the system boundary is defined both logically and physically. Logically, or from an IT services perspective, the scope or boundary of the NOAA0520 system is considered to include the SCADA systems used to monitor and maintain the facilities that NOAA maintains; environmental monitors for the locations that NOAA does not maintain; and the systems used to support those applications.

b) System location

Physically, the scope or boundary of the NOAA0520 system is considered to include all of the following data center locations:
Boulder, CO (additional)
Silver Spring, MD (additional)
Ashburn, VA (additional)
Fairmont, WV (primary)

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

Interconnected with NOAA N-Wave for transport services between NOAA0520 locations.

d) The purpose that the system is designed to serve

System provides Physical and Environmental security controls in NOAA Office of the Chief Information Officer (OCIO) Data Centers; assisting in high availability and redundancy with high environmental and physical capabilities. Physical Access Control is a primary mission along with ensuring the Data Centers operate in accordance with DOC and NOAA policies.

e) The way the system operates to achieve the purpose

PII consists of information provided for building and restricted area access, including video data. PII inside of the NOAA0520 system boundary is only accessible by Federal employees and NOAA0520 support contractors for the determination of access and badge coding. C-Cure is an application used to manage and monitor physical access.

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

Two separate cards may be required to gain entry to NOAA offices and work areas:

One, to access the building itself issued by the facility; this is needed to use common areas within the facility. The other is a CAC (or Common Access Card) authorized by NOAA, and issued by a Federal Government office. The EDC Access Request, via a Smartsheets form, should be used to request the issue of a building access card and for adding EDC-managed areas to an existing CAC.

In accordance with applicable security controls, unescorted access to EDC must first be requested utilizing the EDC Access Request, via a Smartsheets form, prior to access approvals. Those individuals who would like unescorted access must supply the requested/required data on the EDC Access Request, via a Smartsheets form. Those requested/required data items are Name, Telephone Number, Job Title. Additionally, information collected from CAC is CAC Number (10-digit), Agency, System CS/CI, Personal ID, Org ID and Org Category. Those requests and associated data supplied
by the user are stored in a database and accessible only by authorized privileged account administrators. The individual-supplied data is used only for identification and coding of their CAC as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees and contractors.

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

Federal Employees responsible for Physical access decisions which includes system owner, information system security officer, data center manager and access controllers. Contractors also have access to information through their role in producing badges or supporting the physical security mission.

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

Personnel with security responsibilities access door access and video data via an isolated workstation that has limited access to both the room and terminal. Access determinations are stored within Smartsheets and are only accessible by those involved in access determinations.

i) How information is transmitted to and from the system

Via email, smartsheets, and via administrative input (workstation) for access determinations. Video data and door access data is transmitted to / from a workstation for security 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.*

____ 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):					

____ 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.*

X___ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact. *Continue to answer 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.

X___ 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.

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

Activities			
Audio recordings		Building entry readers	X
Video surveillance	X	Electronic purchase transactions	
Other (specify): There is video surveillance in EDC facilities which houses NOAA offices and NOAA employees.			

____ 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.

X 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
X Contractors working on behalf of DOC
X 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?

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

_X_ 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

__X__ The criteria implied by one or more of the questions above **apply** to the NOAA Enterprise Data Centers (EDC) 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 NOAA Enterprise Data Centers (EDC) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner
Name: Steven Leigh (ISSO)
Office: NOAA/OCIO
Phone: (771)210-9187
Email: steven.leigh@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: LEIGH.STEVEN.A.1290923979 Digitally signed by LEIGH.STEVEN.A.1290923979 Date: 2023.01.26 15:33:02 -05'00'

Date signed: 9

Information Technology Security Officer
Name: Ansaruddin Hasan
Office: NOAA/OCIO
Phone: 202-964-0871
Email: ansaruddin.hasan@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: HASAN.ANSARUDDIN.ISA.1376816210 Digitally signed by HASAN.ANSARUDDIN.ISA.1376816210 Date: 2023.01.26 17:43:09 -05'00'

Date signed: 6816210

Privacy Act Officer
Name: Robin Burress
Office: NOAA OCIO
Phone: 828-271-4695
Email: robin.burress@noaa.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.02.06 13:11:52 -05'00'

Date signed: .1365847696

Authorizing Official
Name: Douglas Perry
Office: NOAA/OCIO
Phone: (301) 706-8742
Email: douglas.a.perry@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: PERRY.DOUGLAS.ALLEN.1365847270 Digitally signed by PERRY.DOUGLAS.ALLEN.1365847270 Date: 2023.02.02 13:44:01 -05'00'

Date signed: 1365847270

Bureau Chief Privacy Officer
Name: Mark Graff
Office: NOAA OCIO
Phone: 301-628-5658
Email: mark.graff@noaa.gov

I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.

Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.03.07 08:10:23 -05'00'

Date signed: 47892

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.