

U.S. Department of Commerce
NOAA



Privacy Threshold Analysis (PTA)
for
NOAA1200 CORPSRV

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOAA1200

Unique Project Identifier: 006-00035110000-48-02-00-01-00

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).

a, b and c - NOAA1200 / CorpSrv, is a General Support System (GSS) consisting of multiple subsystems. NOAA1200 is hosted in the NOAA network infrastructure and not a standalone system.

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.

- | | | |
|---------------------|-------------------|------------------------|
| 1. Boulder, CO; | 6. Largo, MD; and | 11. Silver Spring, MD; |
| 2. Fairmont, WV; | 7. Newport, OR; | 12. Tampa, FL; |
| 3. Germantown, MD; | 8. Norfolk, VA | 13. Washington, DC. |
| 4. Honolulu, HI; | 9. Norfolk, VA; | |
| 5. Kansas City, MO; | 10. Seattle, WA; | |

NOAA1200 supports a user base of approximately 2,600 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.

d, e, and f - 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. Residual data from other privacy systems may be stored, and/or processed on user workstations or file servers.

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.

g. - NOAA1200 shares data with twelve 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.

The following cloud services are currently administered for the NOAA enterprise under NOAA1200 and will be moved to NOAA0900 FISMA compliance by the end of 3QFY2020.

Unified Messaging Service (UMS) / Google Government Suite (G-STE)

Google Services is comprised of Google's multi-tenant public and hybrid Google Apps cloud instances and multi-tenant public cloud Google App Engine. These services are built atop the Google Common Infrastructure. Google Apps is a Software-as-a-Service (SaaS) cloud deployment model that allows customers the ability to communicate, store files and collaborate with Gmail, Hangouts, Talk, Calendar, Drive, Docs, Sheets, Slides, Vault, Sites, Groups, Contacts and Classroom while managing their domain with the Admin Console.

G-STE completed an assessment and authorization (A&A) under the GSA FedRAMP program. It is authorized as a MODERATE Impact system which is adequate for the NOAA owned data processed and stored there. NOAA1200 users are not authorized to use G-STE for processing and storage of sensitive PII/BII, which is covered in the annual NOAA Information Technology Security Awareness Course (cyber security training).

ServiceNOW

ServiceNow is a suite of natively integrated applications designed to support IT service automation, resource management and shared support services. The ServiceNow platform includes customization tools to help customers create solutions for business requirements. ServiceNOW applications cover all Information Technology Infrastructure Library (ITIL) processes and are natively integrated on a single platform providing web intuitiveness and process automation. ServiceNOW is a modular solution, meaning that customers may use all, or a sub-set of the applications provided via ServiceNow. The ServiceNOW SaaS application is a group of modules, or pages, that provide related information and functionality in a ServiceNOW instance. These SaaS applications can be added or removed by enabling or disabling the application's plugin. ServiceNOW is designed to support processes, tasks, change management, and other IT processes through automation. It is a customizable environment and provides the ability for customers to design and implement applications as part of the ServiceNOW application framework.

ServiceNOW completed an assessment and authorization (A&A) under the GSA FedRAMP program.

Mobile Device Management (MDM) / IBM MaaS360

The IBM MaaS360 is a comprehensive, cloud-based security and management platform for NOAA mobile devices, applications and content. NOAA uses MaaS360 to protect data and optimize productivity, enabling employees to work anytime and anywhere through trusted mobile interactions. MaaS360 provides a cloud based, on-demand software-as-a-service (SaaS) delivery model, built on a secure, multi-tenant architecture.

The Mobile Device Management IBM MaaS360 platform currently allows the use of facial recognition for unlocking mobile devices. This technology utilizes iris and retina scans, and other facial features including the depth, contour and shape of the face, as well as one's gaze to unlock mobile devices. However, users must also establish a passcode which can be used to bypass the facial data to unlock the devices. The biometric data collected by the device is stored, processed and encrypted locally on each device. The collection of the facial images is incidental to the device use. This data will not be collected in a system of record and will not be shared or retrieved by anyone within or outside the bureau. The only exception to this is in cases where the phone data, including the PII data collected by the phone is shared, if necessary, with law enforcement.

The IBM MaaS360 cloud service completed an assessment and authorization (A&A) under the GSA FedRAMP program. MDM Federal Information Security Management Act (FISMA)

AODocs

AODocs is a document management system that will allow NOAA to collaborate on its Google services solution to organize business critical documents, migrate files from legacy document management systems, implement business workflows, manage documents with metadata and apply document retention policies entity-wide. This solution is not yet in use at NOAA, however, in the future it will be used to distribute Standard Operating Procedures, manage quality control processes, and assist in the coordination of contract management, procurements, intranet publication and incident reporting. AODocs will not store any NOAA data on its servers, it will only leverage the Google cloud platform (Google App engine and Google Datastore). Google Drive data will remain in the G suite environment. While AODocs is not FedRAMP certified, it is hosted on the Google infrastructure to deliver its product (G Suite) and backend (Google Cloud Platform), however the operating environment is administered by AODocs.

Smartsheet

Smartsheet is a SaaS application for collaboration and work management that is developed and marketed by Smartsheet Inc. It is used to assign tasks, track project progress, manage calendars, share documents and manage other work. It has a spreadsheet-like user interface.

Smartsheet is in the process of becoming fully implemented beginning 1QFY2020. It is currently undergoing a GSA FedRAMP A&A and at the time of this publication has completed its third party assessment. It is not authorized for processing or storing sensitive PII/BII.

g. Information will be shared 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.

Questionnaire:

1. What is the status of this information system?

This is a new information system.

This is an existing information system with changes that create new privacy risks.

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.

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).

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

Yes. Please describe the activities which may raise privacy concerns. Facial recognition feature on some cell phones, stored only on the phones. Also, there are building entry card readers in the Silver Spring Metro Complex.

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

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

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)?

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

DOC employees

Contractors working on behalf of DOC

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?

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?

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, 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.

CERTIFICATIONS

X I certify the criteria implied by one or more of the questions above apply to the NOAA1200 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 NOAA1200 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

RICKETT.JASON.ALLEN.139239295 Digitally signed by
1 _____ RICKETT.JASON.ALLEN.1392392951
Date: 2019.10.23 15:49:25 -04'00'

System Owner (SO): Jason Rickett (In lieu of) **CAMERON SHELTON**

OBENSCHAIN.CHARLES Digitally signed by
.THOMAS.1506347293 **OBENSCHAIN.CHARLES.THOMAS.**
1506347293
Date: 2019.10.25 09:12:26 -04'00'

Information Technology Security Officer (ITSO): **CHARLES OBENSCHAIN**

PERRY.DOUGLA Digitally signed by
S.A.1365847270 **PERRY.DOUGLAS.A.1365847270**
Date: 2019.10.25 13:52:44 -04'00'

Authorizing Official (AO): **DOUGLAS A. PERRY**

_____ Bureau Chief Privacy Officer (BCPO): **MARK GRAFF**

GRAFF.MARK.HYR Digitally signed by
UM.1514447892 **GRAFF.MARK.HYRUM.1514447892**
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2019.10.28 16:42:40 -04'00'