Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
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).

Description of the information system and its purpose:
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 subsystems associated with NOAA1200 are:

Subsystem Type	Subsystems
Cloud Systems	Google Government Suite ; IBM Maas360, SkyHigh Networks CASB (Not yet operational); AODocs (Not yet operational)
Major Applications	C-CURE; FedSelect; OMAO Waypoint Global Doc Management; HS EOC Backup
Sharepoint	NMFS HQ's; Deep Water Horizon (DWH); WFMO; NOAA OCIO

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;
2. Fairmont, WV;
3. Germantown, MD;
4. Honolulu, HI;
5. Kansas City, MO;
6. Largo, MD; and

7. Newport, OR;
8. Norfolk, VA
9. Norfolk, VA;
10. Seattle, WA;
11. Silver Spring, MD;
12. Tampa, FL;
13. Washington, DC.

NOAA1200 supports a user base of approximately 3,000 users, and provides connectivity to the NOAA network for both local and remote access to the following basic administrative services: collaboration platforms includes Google Suite for government cloud, file servers, printing; file backup and restoration; and account management and storage.

d, e, and f - NOAA1200 workstations allows Application Information System (AIS) users (including Trusted Agents) to connect to other 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, photographs, 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.

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. Google App Engine is a Platform-as-a-Service (PaaS) cloud deployment model, providing an environment to build, run and manage applications on Google's infrastructure.

G-STE is assessed and authorized (A&A) under the Federal Risk and Authorization Management Program (FedRAMP), administered by the US GSA. 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).

Mobile Device Management (MDM) / IBM MaaS360

The IBM MaaS360 is a cloud-based security and management platform for NOAA mobile devices, applications and content. NOAA uses MaaS360 to protect data providing the ability 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 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.

MDM Federal Information Security Management Act (FISMA) Risk Management Framework (RMF) Assessment and Authorization (A&A) are met via FedRAMP.

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 will rely on Google infrastructure to deliver its product (G Suite) and backend (Google Cloud Platform). Google is FedRAMP certified.

SkyHigh

NOAA has acquired SkyHigh Cloud Access Security Broker (CASB) to implement Data Loss Prevention (DLP), which will be utilized to enforce PII policies for data at rest stored on NOAA's Google Drive. SkyHigh will perform scans of data files stored on the Google Drive to identify data in violation of privacy policy. SDD DLP Administrator and NOAA POCs are working with the SOC and NCIRT to determine what actions will be taken upon notification of a PII policy violation from the DLP engine. PII policy violation log information will be sent to Arcsight in real time in collaboration with the NOAA SOC. Skyhigh FISMA RMF A&A are met via FedRAMP.

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.

h & i. Data is retrieved and transmitted via network resources, with the data encrypted before transmission. The network resources require user authentication, via the use of CAC cards. Applications use encryption as well as application authorization via roles and privileges. Emails are only directed to specific recipients and or gatekeepers.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system.
__X__ 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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): The existing changes to the NOAA1200 will result in an increase in the sensitive PII, facial and biometric data processed by the system. The sensitive PII data reside within the hosted system networks and locally on users workstations. The facial data from the mobile devices will be stored on mobile devices if selected. Skyhigh and AODocs are future subsystems not yet operational. In addition, 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, photographs, 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. There are building entry card readers in the Silver Spring Metro Complex.					

____ 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 01-2015 or later).

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

__X__ 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)?

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

____ Companies

__X__ 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)?

__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__ 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?

__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.

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?

__X__ 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.

CERTIFICATION

___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 [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): [ISSO for] **CAMERON SHELTON**

GRIGSBY.THOMAS.W.1049202896

Digitally signed by GRIGSBY.THOMAS.W.1049202896
Date: 2018.03.08 14:44:27 -05'00'

Signature of SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): **JEAN APEDO**

APEDO.JEAN.1188076064

Digitally signed by APEDO.JEAN.1188076064
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=APEDO.JEAN.1188076064
Date: 2018.03.09 09:25:46 -05'00'

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO): **DOUGLAS PERRY**

PERRY.DOUGLAS.A.1365847270

Digitally signed by PERRY.DOUGLAS.A.1365847270
Date: 2018.03.09 13:48:30 -05'00'

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): **MARK GRAFF**

GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.03.09 14:13:[illegible] -05'00'

Signature of BCPO: _____ Date: _____
