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

Privacy Threshold Analysis for the
NOAA0900
Consolidated Cloud Applications (CCA)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/OCIO/Consolidated Cloud Applications (CCA)

Unique Project Identifier: NOAA0900

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:

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).

NOAA0900 is a consolidated accreditation boundary for multiple existing NOAA cloud applications, as well as any new cloud applications. NOAA Consolidated Cloud Applications' component cloud applications are distributed among multiple Cloud Service Providers (CSP).

This is an aggregated system with multiple applications, which are connected through NOAA networks to various Cloud service Providers. These applications are as follows:

Everbridge Suite (EBS)

EBS is a Software-as-a-Service platform that is used for managing critical events. Federal Agencies and other organizations use EBS platform for operational response to critical events in order to keep people safe and businesses running faster. During public safety threats such as active shooter situations, terrorist attacks or severe weather conditions, as well as critical business events such as IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, customers rely on the EBS platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes, and track progress on executing incident response plans. Many Federal agencies utilize EBS as part of their employee communication strategy – for agency's contingency planning and business continuity, staff augmentation, and IT Alerting needs.

Google Workspace

Google Workspace is a collection of cloud computing, productivity, and collaboration tools,

software and products. It includes email, calendar, contacts, chat, drive, and meet for users.

Maas 360

MaaS360 configures mobile devices using the DoD Security Technical Implementation Guide (STIG) cybersecurity baseline. MaaS360 offers scale, control and security across all devices and mobile platforms, providing total device management by user, device, application, and across an enterprise. As a fully integrated cloud platform, MaaS360 delivers Mobile Device Management (MDM) to customers.

ServiceNow

The ServiceNow product is a suite of natively integrated applications designed to support IT service automation, resource management and shared support services. ServiceNow is built on modern web technologies. The ServiceNow platform includes easy-to-use, point-and-click customization tools to help customers create solutions for unique business requirements.

SmartSheet

SmartSheet provides a cloud collaboration platform to enable users to plan, capture, manage, automate, and report on work while utilizing various collaboration features. SmartSheet projects provide essential tools for project management.
Smartsheet collects the following information: Administrative Data; Financial Administration (IT Acquisition workflows); IT Ticket System (Help Desk); and Project/Program Management.

Ivanti

Ivanti Service Manager (ISM) is a cloud-based IT Service Management (ITSM) solution. ISM is designed to be the central point of contact between users, employees and the IT organization. It offers first and second line support to users, where incidents, problems or inaccuracies in IT systems are reported.

AODocs

AODocs is a document management system which is used distribute Standard Operating Procedures, manage quality control processes, and assist in the coordination of contract management, procurements, intranet publication and incident reporting.

Esri

Esri is an international supplier of geographic information system (GIS) software, web GIS, and geodatabase management applications. There are several custom applications, mostly web-based, that are used to input, process, and provide access to a myriad of scientific and administrative data.

Esri, a geospatial cloud which hosts ArcGIS data as web layers, allows complex datasets on easy-to-understand smart maps, which are used to visualize and monitor important trends across lines of business and take action in mission-focused projects. A geospatial cloud also allows location intelligence data to be easily combined with artificial intelligence and predictive analytics to map out ways to drive productivity or adjust strategies before bigger problems develop.

CloudCheckr

The CloudCheckr system is a cloud cost and security management tool that allows companies to review cost, inventory, security, compliance, and utilization information about their cloud environments. Customers can drill down for more information on each check, customize the CloudCheckr dashboards that are displayed, set up alerts and notifications, or create and export reports.

Avaya One Cloud

Avaya OneCloud For Government is a family of real-time and near-real-time enterprise-grade applications for Unified Communications, Contact Center/Customer Experience (CX) and voice/video/web collaboration. The solution is comprised of the following elements as part of the standard offering:
- MPLS network as transport (or optional 3rd party transport – agreed upon between Avaya and said Agency) provided by Service Provider partners
- Avaya OneCloud For Government Hosting Facilities
- Avaya OneCloud For Government Network Operations Centers (NOCs) - Avaya facilities in Columbia, MD and Coppell, TX
- SIP Trunking to the PSTN (via existing agency carrier) for inbound and outbound PSTN calling
- CPE - Installation and Maintenance Options
- Optional customized solutions to integrate into Government customer environments

Qualtrics

Qualtrics is a simple to use web-based survey tool to conduct survey research, evaluations and

other data collection activities.

Entellitrak

Entellitrak is an enterprise level COTS (Commercial Off-The-Shelf) that provides unified BPM software by using an open architecture approach that focuses on the core technologies that streamline work for rapid application development on business processes. Entellitrak provides all of the functionality required to collect, track, manage, process, and report on information regarding a business process.

NOAA0900 does collect and display photographs of employees and contractors on some websites in support of education and outreach. Notice and consent is provided prior to collecting, storing, and using these images.

Address the following elements:

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

NOAA0900 is a General Support System.

b) *System location*

NOAA OCIO offices are located at the Silver Spring Metro Center (SSMC) campus in SSMC3 at 1315 East West Highway, Silver Spring, Maryland

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

This is an aggregated system with multiple applications, which are connected through NOAA networks to various Cloud service Providers. These applications are as follows:

Application Names	ATO status	FIPS-199 Categorization
Everbridge Suite (EBS)	FedRAMP ATO	MODERATE
Google Workspace	FedRAMP ATO	HIGH
Maas360	FedRAMP ATO	MODERATE
ServiceNow	FedRAMP ATO	HIGH
SmartSheet	FedRAMP ATO	MODERATE
Ivanti	FedRAMP ATO	MODERATE
AODocs	NOAA Approved	MODERATE
Esri	FedRAMP ATO	LOW
CloudCheckr	FedRAMP Ready	MODERATE
Avaya One Cloud	FedRAMP ATO	MODERATE

Qualtrics	FedRAMP ATO	MODERATE
Entellitrak	FedRAMP ATO	MODERATE

d) *The purpose that the system is designed to serve*

This system provides a variety of applications to support the overall NOAA mission.

These applications range from document processing, storage, and retention, weather and mapping, to emergency notification systems.

e) *The way the system operates to achieve the purpose*

As the system is an aggregate system, NOAA0900 provides overall management and security support.

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

EBS collects the following information: name, work phone number, work cell phone number, work email address, work mailing address, organization data, and account data.

Google Workspace collects email logs, authentication logs, basic user information, device information, calendar logs, and drive logs. Data Owners (customers) determine what content is stored in Google Workspace and with whom that content is shared.

MaaS360 collects basic user information and basic device information. MaaS360 does not collect PII or BII.

ServiceNow collects user information such as name, user information related to injuries, deaths, incident information, and mishaps that occur to those users, and IT Ticket information. Data Owners (customers) determine what content is stored in ServiceNow and with whom that content is shared.

Smartsheet does not collect PII or BII. Data Owners (customers) determine what content is stored in SmartSheet and with whom that content is shared.

Ivanti does not collect BII or PII.

AODocs: Commerce Alternative Personnel System (CAPS) performance evaluations, safety and protocol documents related to marine operations, marine engineering drawings and correspondence, and other generic file-sharing repositories.

Esri collects basic organizational profile information such as username, email, and a biography. Esri does not collect any PII or BII.

CloudCheckr does not collect any PII or BII.

Avaya One Cloud collects Name, Phone, Number, Email, Location, and Voicemail.

Qualtrics: Survey Owners (customers) determine what content is stored in Qualtrics and with whom that content is shared.

Entellitrak PII collected in the system consists of: employee's or applicant's name, functional limitation caused by the disability, reasonable accommodation (RA) requested, explanation of how RA would assist the applicant in the application process or the employee in performing his/her job or receiving the benefits and privileges of employment, dates when the required interactive discussions were held, notes from discussion regarding the request, action by deciding official, whether medical documentation was sought, justification for requesting medical documentation, any sources of technical assistance that were consulted, and if the request was denied, the reason for denial (but not medical documentation, which will be kept in a separate file).

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

Access is restricted, requiring authorized users, those with a "need to know", to log in.

These include system staff and contractors.

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

NOAA0900 applications information is accessed by authorized personnel in order to deliver a variety of support information. Users authenticate via NOAA ICAM (Identity, Credential, and Access Management Services).

i) *How information is transmitted to and from the system*

NOAA0900 applications information is accessed by authorized personnel via NOAA networks and multiple CSPs in order to deliver a variety of support information. All traffic is encrypted during transit utilizing FIPS-140-2 compliant cryptographic modules.

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 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.

_X_ 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.

_X_ Yes. _(Check all that apply.)_

Activities			
Audio recordings	X	Building entry readers	
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.)."

  X   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."

  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
          Other Federal Government personnel
    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 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.   Medical records are imported into the AODocs library containing Protected Health Information (PHI) or PII such as full name, SSN, date of birth and email address.
Provide the legal authority which permits the collection of SSNs, including truncated form.   The authority for the collection of this data is Federal Continuity Directive 1, Code of Federal Regulations, Title 41, Chapter 102 Federal Management Regulation (FMR), Part 102-74 (41 CFR §102-74.230 - 102-74.260), DOC's Departmental Organizational Order (DOO) 20-6, and guidance provided by DOC's Manual of Security Policies and Procedures, Chapter 7.   Applicable SORNs are as follows: ● COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons   ● COMMERCE/DEPT-13, Investigative and Security Records

- COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
- COMMERCE/DEPT-25, Access Control and Identity Management System
- GSA./GOVT-7, HSPD-12 USAccess
- OPM/GOVT-1, General Personnel Records

_____ 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 NOAA0900 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 NOAA0900 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner	**Information Technology Security Officer**
Name: Stefan Anton Leeb Office: NOAA OCIO Phone: 301.628.5109 Email: Stefan.leeb@noaa.gov Signature: _LEEB.STEFAN.ANTON.1158781260_ Date signed: 2023.01.12 17:36:03 -05'00'	Name: Ansaruddin Hasan Office: NOAA OCIO Phone: 240-255-8556 Email: Ansaruddin.Hasan@noaa.gov Signature: HASAN.ANSARUDDIN.ISA.1376816210 Digitally signed by HASAN.ANSARUDDIN.ISA.1376816210 Date signed: 2023.01.13 08:12:39 -05'00'
Privacy Act Officer	**Authorizing Official**
Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov Signature: BURRESS.ROBIN.SURRETT.136584 7696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date signed: 2023.01.30 10:48:10 -05'00'	Name: Douglas Perry Office: NOAA OCIO Phone: 301.713.9600 Email: douglas.a.perry@noaa.gov Signature: PERRY.DOUGLAS.ALLEN.1365847270 Digitally signed by PERRY.DOUGLAS.ALLEN.1365847270 Date signed: 2023.01.23 11:30:32 -05'00'
Bureau Chief Privacy Officer	**Information System Security Officer**
Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date signed: 2023.02.07 08:10:43 -05'00'	Name: Mustafa Lutfi Office: NOAA OCIO Phone: 202-964-0589 Email: Mustafa.Lutfi@noaa.gov Signature: LUTFI.MUSTAFA.FAROUK.FOUAD.1368390476 Digitally signed by LUTFI.MUSTAFA.FAROUK.FOUAD.1368390476 Date signed: 2023.01.12 14:33:40 -05'00'