U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA0900 Consolidated Cloud Applications

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 03/04/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment NOAA0900/Consolidated Cloud Applications

Unique Project Identifier: 006-48-02-00-02-0000-00

Introduction: System Description

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). NOAA OCIO offices are located at the Silver Spring Metro Center (SSMC) campus in SSMC3 at 1315 East West Highway, Silver Spring, Maryland and is a General Support System.

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
G Suite	FedRAMP ATO	MODERATE
Maas 360	FedRAMP ATO	MODERATE
ServiceNow	FedRAMP/NOAA ATO	HIGH
SmartSheet	FedRAMP ATO	MODERATE
Ivanti	NOAA approved, FedRAMP Ready	MODERATE
AODocs	NOAA Approved/FedRAMP Moderate in Process	MODERATE/ FedRAMP MODERATE in process
MS Dynamics	DOC approved ATO	HIGH
Esri	FedRAMP (Dept of Interior approved) ATO	Low
Virtru	FedRAMP ATO	Moderate

See respective NOAA0900 component applications PIA documentation contained in applications' ATO packages for specific details on information collected.

EBS: Everbridge Suite (EBS) is a Software-as-a-Service platform that is used for managing critical events. Federal Agencies and other organizations use the EBS platform for operational response to critical events in order to keep people safe and businesses running effectively. 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, the EBS system functions 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. It is built on multi-tier architecture within Amazon Web Services' public cloud infrastructure in East/West regions which are FedRAMP compliant.

EBS collects the following Personally Identifiable Information (PII): name, work phone number, work cell phone number, work email address, and work mailing address.

G Suite: Google Suite, a PaaS provider, supplies mail/calendar and Google drive services to all NOAA staff, is also integrated into NOAA0900.

The Google Services offering consists of two primary layers; Google Cloud Platform (GCP) and Google Common Infrastructure (GCI). The Google Cloud Platform contains 49 customer facing services. The services within the Google Cloud Platform sit on top of Google Common Infrastructure, which is infrastructure private to Google that is responsible for the implementation of common controls for all Google service offerings. These two pieces work together to provide the Google Services offering.

GCP is an extensive suite of products from Google-controlled development environments (e.g. Google App Engine) to customer-managed environments (e.g. Google Compute Engine) offering flexibility via fully customizable virtual machines and utilization of other services like `

- fully-managed databases and data analytics tools,
- networking services including virtual load balancing and virtual private cloud solutions,
- access management tools,
- cloud project management tools,
- machine learning capabilities, and developer tools.

GCI is private infrastructure, utilized only by Googlers and Google-developed software, while GCP is a public hybrid cloud that is hosted on GCI, serving the US Federal Government, personal users, and other organizations. GCI is responsible for implementation of common controls for all Google service offerings, including GCP. Customers have no direct access to GCI, but interaction with Google's IaaS/PaaS/SaaS offerings (like GCP) result in traffic and data in GCI.

Google maintains a private cloud Infrastructure as a Service (IaaS), GCI, upon which its product offerings are built. Per the NIST SP 800-145 definition of a Private IaaS Cloud, the GCI is restricted to Googlers and consists of multiple reusable services such as databases, compute services, management tools, and security controls of which all Google services can take advantage. Abstracting these components to a common layer means that Google can apply consistently strong data protection and security controls across all service offerings. In addition to providing a technical infrastructure for products to run, GCI provides common processes such as security training, change management, secure software development lifecycle (SDLC), vulnerability management, and risk management. This is fundamentally different from the way other companies develop software and gives Google an advantage when it comes to uniform management of its products where each product inherits security technology, controls and processes from GCI. Google Cloud Platform runs on top of the Google Common Infrastructure. The Google Common Infrastructure consists of four components:

- Network,
- Data centers,
- Resource management, and
- Data Storage

The GCP is comprised of IaaS, PaaS and SaaS offerings that sit on top of Google Common Infrastructure. GCP offers a combination of services ranging from a fully customer managed virtual infrastructure and associated storage/DB and networking services that allow customers to provision fundamental computing resources from the operating system up the technology stack (Google Compute Engine) (IaaS), to a CSP-managed platform for deploying applications onto the cloud without having to manage the underlying infrastructure (Google App Engine) (PaaS), to system management tools and advanced Machine Learning API's.

G Suite collects email logs, authentication logs, basic user information, device information, calendar logs, and drive logs. G Suite collects PII and BII.

MaaS 360: 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.

MaaS360 collects basic user information and basic device information. The Mobile Device Management (MDM) 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 overall system categorization of MaaS360 is MODERATE.

MaaS360 does not collect PII or BII.

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 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.

The overall system categorization of ServiceNow is HIGH. ServiceNow has a JAB Provisional Authorization date of August 12th, 2019.

ServiceNow collects PII in the form of vehicle identification numbers that are collected in the NOAA Safe application when an accident occurs involving a vehicle.

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.

Various features within the application include project tracking, smart grids, calendars, dashboards, cards, portals, forms, automations, and control center.

Smart projects allow users to manage every aspect of complex projects, and visualize tasks in Gantt, card, and calendar views. Smart grids provides a unified, customized view of projects that keeps teams on task and on time to easily track multiple moving parts. Smart calendars keep teams in sync with an interactive, comprehensive view of all activities and critical timelines. Smart dashboards provide project owners and stakeholders a real-time view into the status of top key performance indicators, critical trends, and summary reports. Smart cards give teams a more visual way to communicate and collaborate in Smartsheet. Smart portals bring teams together and keep them on the same page with an easy-to-create and maintain centralized information portal. Smart forms empower business users to speed execution and foster innovation by making it easy to collect and act on data. Smart automations put simple and powerful work process automation rules to work in a matter of minutes.

Smartsheet utilizes two (2) AWS VPCs (Management VPC and Product VPC) to control communications to the Smartsheet Gov. environment. The external boundary is monitored and controlled at three separate locations, two access paths (bastion host and Windows jump host) and for the Management VPC and one access path (AWS ALBs) to the Product VPC. The Management VPC is accessible only to Smartsheet personnel via strict routable access (Corporate IP whitelisting) and a valid access authorization. Smartsheet administrators utilize an OpenSSL VPN (TLS 1.2) from the corporate network to connect to a jump host (AD + YubiKey credentials) in the Management SG. The Bastion Host is a Red Hat Enterprise Linux (RHEL) Server configured with FIPS 140-2 validated modules (please see SC-8 for certificate numbers) for OpenSSH and OpenSSL. From the bastion/jump host, administrators can either RDP or SSH to the instance they need to manage within the Smartsheet Gov. environment. Access to the Product VPC is restricted to HTTPS only and is routed through AWS ALBs to handle the TLS termination of customer sessions to the Smartsheet Gov. Application.

Within the Management VPC each application is within its own AWS Security Group. For example, the vulnerability scanning tool and Sherlock ELK are separated into dedicated AWS SGs. Similarly, within the Product VPC each component supporting an application such as Core App is separated into AWS SGs. Individual components performing the same function are grouped within the same AWS SG (i.e. Core APP RDS DBs). Communication between the Management VPC and the Product VPC is accomplished via AWS VPC peering. All authentication across the boundary requires an MFA token.

Smartsheet Gov. connects to an array of corporate services and a single external service. Smartsheet utilizes Lucidchart to create the initial set of diagrams. There is no connection between Lucidchart and Smartsheet Gov. Smartsheet has a contract with DocuSign to handle customer acknowledgement and signature acquisition prior to onboarding personnel. NetSuite is deployed within the corporate environment and is utilized for enterprise resource planning. Salesforce is utilized by Smartsheet corporate personnel to manage financial relationships with customers and perform customer relationship management (CRM). Slack has been implemented to support interoffice communications. Finally, Gmail is used for general email services within the corporate environment. Smartsheet enforces via policy to prevent the communication of customer data and/or information within corporate services.

The single external service for the Smartsheet Gov. environment is PagerDuty. Smartsheet contracts with PagerDuty to perform alerting of relevant Smartsheet Gov. Points of Contact (POC) for escalating issues within the environment. No sensitive or customer data is sent through the PagerDuty alerts. PagerDuty alerts send only the message that the relevant users must log into the Smartsheet Gov. environment to check on the status of an emerging incident.

Smartsheet collects the following information:

- Administrative Data

- Financial Administration (IT Acquisition workflows)
- IT Ticket System (Help Desk)
- Project/Program Management

Smartsheet does not collect PII or BII.

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. ISM can also be an important source of management information for reporting and auditing purposes. ISM fully supports Incident, Problem, Change and Release Management, Self-Service, & 3rd party integration. Ivanti's software is used by FSD (Finance Systems Division) to provide and monitor help desk support and manage internal FSD configuration and management requests.

The authorization boundary of the ISM consists of the AWS East/West Virtual Private Cloud (VPC) to host multi-tenant environments, an Ivanti Management VPC to host management and security tools, AWS Management Console for administration of the of the multi-tenant environments, and external cloud systems to support the ISM production environment such as Qualys Cloud. Additionally, Ivanti includes AWS services such as EC2, S3, CloudTrail, and etc. to be in the authorization boundary. These virtual system environments within AWS, AWS services, and external cloud systems constitute the authorization boundary by Ivanti as they store, process, and/or process customer information.

The system components that make up ISM are hosted within the AWS US East/West data center facilities. Ivanti relies on AWS to provide appropriate physical and logical protections and processes for the AWS datacenter facilities. For the purposes of FedRAMP, the AWS datacenter facility will be considered a leveraged, authorized service provider. The AWS datacenter facility will not be assessed by the 3PAO during assessment activities.

Customer users are able to log into their ISM web application tenant environment using their own organization credentials. Using SAML technology, customers can federate their web application to their internal account management infrastructure to access the ISM environment. This access method includes the acceptance of PIV/CAC credentials.

The ISM authorization boundary does not currently have any dedicated interconnections between other information systems within the authorization boundary for purposes of storing, processing, and transmitting Federal customer data. External system connections not used to store, process, or transmit federal data but used for management or operation services are implemented and managed in accordance with the acquisition process described in SA-4 and SA-9. Additionally, all external connections will adhere to FedRAMP requirements for periodic risk assessments to identify potential risk posed by such connections.

For current operational and management external connections, Ivanti works with the external vendor to ensure appropriate protections are in place based on the service. Ivanti will also maintain data confidentiality and support data integrity as applicable to the external service.

ISM is hosted within AWS US East/West and uses the Virtual Private Cloud (VPC) service to define the ISM authorization boundary. The AWS VPC is completely logically separated from other customers hosted within the AWS environment. The VPC ensures that sensitive resources and data are completely isolated and secured.

Ivanti does not collect BII or PII.

AODocs: AODocs is a document management system which is used to distribute Standard Operating Procedures, manage quality control processes, and assist in the coordination of contract management, procurements, intranet publication and incident reporting. While AODocs is not FedRAMP certified, it is hosted on Google's G Suite infrastructure that is FedRAMP certified and included in NOAA’s Google ATO, and Google Cloud Platform, which is also FedRAMP certified, but has not been approved for use under NOAA’s Google ATO. AODocs is the subject of a PL-2 POA&M which requires a full NOAA ATO evolution to be conducted on the application. AODocs has not been vetted through the ATO process. This application contains various Human Resources data items. A risk assessment was completed on May 12, 2017 and a memo to approve AODocs for NOAA usage was approved October 20, 2017.

The following information is collected in 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.

AODocs collects PII and BII.

MS Dynamics: Microsoft Dynamics, cloud solution is a line of enterprise resource planning and customer relationship management software applications. It is a Point of Sale System at the Boulder Warehouse.

Dynamics 365 is a Customer Relationship Management (CRM) software package developed by Microsoft. With Dynamics 365, Microsoft is providing Dynamics 365 functionality (the boxed product and the SaaS product share the same codebase) in the cloud, through a Software as a Services (SaaS) cloud service model. The Dynamics 365 SaaS model allows users to coordinate workflow and develop metrics for the sales and marketing efforts within an organization. Dynamics 365 is deployed within Microsoft datacenters in a manner consistent with a multi-tenant, public cloud deployment model. Due to demand from government customers, Dynamics 365 created a physically and logically separate community cloud environment specifically for government customers in order to meet government expectations for system administrative control and data protections. Dynamics 365 for Government relies on several other Microsoft government-focused cloud information systems to provide physical security, infrastructure, and platform services for the application environment (the information system).

MS Dynamics collects information on Natural Resource Damage Assessment (NRDA), restoration cases, associated financial data on receipts, allocations, obligations, expenditures, transfers, adjustments, and indirect rates.

The purpose of MS Dynamics is to track financial information on cases/projects provided at a level of granularity not available within the NOAA financial system.

The overall system categorization of MS Dynamics is HIGH. MS Dynamics is DOC approved and stores and transmits BII

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. With a geospatial cloud, maps can be created that represent thousands of relationships between hundreds of layers of data on demographics, sales, population growth, likely customers, competitors, supply chains, delivery routes, and countless other variables.

ArcGIS Online includes a wide range of apps that allows interaction with maps and data. Organization members can use their site's app launcher to open apps and related Esri websites that are available to them. Apps include:

Apps for the field - Provide focused workflows and tools for your day-to-day tasks. With these apps, you can track assets, create operational dashboards, collect data and imagery, and navigate routes.

Apps for the office - View, analyze, create, and share maps and location information. ArcGIS apps work for marketing, operations, strategy, sales, leadership, IT, GIS, and more.

Esri ArcGIS Online’s accreditation boundary consists of a group of virtual machines and services that reside in Amazon Web Services (AWS) and Microsoft Azure. These virtual machines include web services, application and data services. AGO is interconnected with SalesForce and Esri Internal Systems (AGO Consumption Portal), both of which have interconnection agreements in place with ArcGIS Online.

Esri collects basic organizational profile information such as username and email.

Esri does not collect any PII or BII.

Virtru: Virtru is an email encryption and digital privacy company.

The VDP Platform service provides client-side encryption of emails and files within a customer's environment. Major VDP functions and components include:

The Virtru client, which is available as plugins or extensions for Google G Suite, Microsoft Office 365 (O365), and Outlook email applications and Google Drive. Versions for mobile device operating systems such as iOS and Android are also available. Virtru plugins provide the functionality to run data loss prevention (DLP) rules and to encrypt emails and files before leaving the client.

The Secure Reader, which provides a web interface for recipients who do not have one of the Virtru clients installed to decrypt Virtru secure messages or files and reply with encrypted messages.

The Virtru Dashboard, which provides a web interface for users and administrators to review and manage secure message policies, user licenses, and data loss prevention (DLP) rules for their account. A command line interface (CLI) version of the dashboard is available as well.

The VDP Platform uses the Trusted Data Format (TDF) to support persistent protection of all content types, including emails, documents, and other data types. Originally developed by the U.S. National Security Agency (NSA) to secure sensitive government data, TDF is an open source format for placing a secure wrapper around any type of content and its accompanying metadata, including metadata assertions (policy-related requirements that allow a content creator to set and enforce a wide variety of policies on the content being provided to the recipient, such as expiring the recipient's access to the content at a certain date and time and allowing or disallowing forwarding of content by recipients).

TDF uses key wrapping, also known as envelope encryption, to encrypt the data encryption key. Envelope encryption is a form of symmetric key encryption that encapsulates (encrypts) cryptographic key material. The Virtru client application uses a secret key to encrypt the customer's email and attachments individually with TDF using AES-256 encryption. The Virtru client encrypts a copy of the email and attachments using a second secret key via TDF. A separate key, known as a Split Knowledge Key, re-encrypts the payload key with TDF. The encrypted content and the Split Knowledge Key are sent to the message recipient and the Access Control key, encrypted Payload Key, and encrypted content are sent to the Virtru Access Control Manager (ACM) and object stores. All encrypted content and keys are sent over TLS using Elliptic Curve Diffie-Hellman Exchange (ECDHE) using Perfect Forward Secrecy (PFS), which provides strong security by ensuring that the connections session establishment keys are ephemeral. All encrypting and decrypting of customer emails and files takes place on the client side using Virtru encryption libraries. Virtru cannot decrypt content as Virtru does not have access to the sender or receiver's email servers. Recipients with the Virtru client decrypt content using the original key in Virtru ACM. Recipients that do not have the Virtru client decrypt the content through the Secure Reader using the Split Knowledge Key.

The Google Drive client works in the same manner, encrypting files using TDF on the client side; however, files are only encrypted with the Access Control Key. The encrypted file is stored in Drive and the Access Control Key is stored in the Virtru ACM.

Initial authentication of a new Virtru user who can encrypt their data using the VDP application occurs via the user's identity provider (IdP). The Virtru client application is connected to the user's domain, so subsequent authentication of the sender occurs through the IdP. The user activation data flow is described in Figure 10-5.

The VDP Dashboard and Secure Reader are the only application interfaces available to end users. The Dashboard provides a web interface for users and admins to review and manage secure message policies, user licenses, and DLP rules for their organization. The Secure Reader allows email receivers without the Virtru client to read and reply to secure emails or Drive users to view files. End users authenticate to the Dashboard and Secure Reader using the identity federation services from their IdP or email service.

The Virtru Administrator Panel (Admin Panel) is a dashboard used by the Virtru Customer Success team for customer support. Virtru personnel authenticate to the Admin Panel via OAuth from the Virtru corporate G Suite domain which leverages Okta for SSO.

Virtru also offers customers on premise security products that can be integrated with the SaaS Offering:

Customers are offered the capability to host a key server in their own network, called a Customer Key Server (CKS). Customers may choose to implement a CKS to add an extra layer of privacy by encrypting object encryption keys with a CKS public key. The customer then holds the private key needed to decrypt the object encryption keys.

Customers are offered network protection of emails to compliment the Virtru plugin client-side protections through the use of the Virtru Email Gateway. The Gateway is placed in-line with established mail flows to run DLP rules before emails leave the network. DLP rules can be set to encrypt the message and set a policy (expiration, disable forwarding, etc.) on the message. The Email Gateway also enables users in a domain to send encrypted emails without installing the client-side plugin.

These Virtru products are provided as Docker containers and are installed on customer owned and managed infrastructure. These software products are integrated in Virtru's SDLC and continuous monitoring activities (including scanning and vulnerability remediation). Virtru releases security updates and notifies customers of available updates. Customers are responsible for authorizing Virtru on-premise products in their environments and for applying updates when released by Virtru.

Virtru also offers an encrypted search functionality which will enable users to perform searches in the inbox for encrypted emails. This feature is disabled by default and can be enabled by organizational administrators in the Virtru Dashboard at any time. When enabling encrypted search, administrators will be warned that they need to fully understand the functionality prior to enabling and link them to the encrypted search FAQ. Customers may want to discuss with their Virtru account manager as well prior to enabling the feature.

Virtru does not collect PII or BII.

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:

- Department-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons (https://www.osec.doc.gov/opog/privacyact/sorns/dept-1.html)
- Department-2, Accounts Receivable (https://www.osec.doc.gov/opog/privacyact/sorns/dept-2.html)
- Department-7, Employee Accident Reports (https://www.osec.doc.gov/opog/privacyact/sorns/dept-7.html)
- DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies (http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html)
- DEPT-25, Access Control and Identity Management System (http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html)
- NOAA-22 NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSO) (https://www.omao.noaa.gov/learn/marine-operations/about/project-planning/health-screening)
- OPM/GOVT-1, General Personnel Records (https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf)
- OPM/GOVT-2, Employees Performance File Records (https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-2-employee-performance-file-system-records.pdf)

This is a HIGH impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

______ This is a new information system.

__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging	X	g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes	X	f. Commercial Sources		i. Alteration in Character of Data	

j. Other changes that create new privacy risks (specify): NOAA0900 has merged the following applications under NOAA0900 which may or may not contain PII and BII: EBS, G Suite. MaaS360, SmartSheet, Ivanti, AODocs, MS Dynamics, Esri, and Virtru.

AODocs, has not been vetted through the Authorization to Operate (ATO) process. This application contains various Human Resources data items.

____ 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.)

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID	X	i. Credit Card	
b. Taxpayer ID	X	f. Driver's License		j. Financial Account	X
c. Employer ID	X	g. Passport		k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): Human Resources information, Personnel Action information					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Human Resources matters including performance appraisals, bonus structures, pay issues, disciplinary actions. Each PII piece is shared with the LO that NOAA0900 is hosting their application for and any subsequent sharing is identified in their individual PIA. MS Dynamics tracks financial information on cases/projects provided at a level of granularity not available within the NOAA financial system. Medical records are imported into the AODocs library and protected using Virtru and the Google Common Infrastructure. AODocs may contain Protected Health Information (PHI) or PII such as full name, SSN, date of birth and email address.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth	X	n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	

b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	X
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

EBS - EBS has implemented measures designed to secure personal information from accidental loss and from unauthorized access, use, alteration and disclosure. The security of your personal information and our customers' information is extremely important to us. When you enter sensitive information and/or geo-location data, we encrypt the transmission of that information using up-to-date security technology (e.g. TLS). https://www.everbridge.com/about/legal/privacy-notice/

MaaS360 - Information is transmitted to and from the system in accordance with its FedRamp authorization using the MaaS360 web portal using HTTPS

ServiceNow - Information is transmitted to and from the system via a secure website. The URL is: https://nsdesk.service-now.com/

MS Dynamics - Information is transmitted to and from MS Dynamics via a restricted secured zone under Microsoft 365 GCC (NOAA SDD tenant space). Data is encrypted.

AODocs - SOC Type 2 system and organizational controls are implemented in cases where customer data is stored. Audits are conducted by an independent third-party public accountant who verifies that Altirnao has the appropriate protections, procedures and policies in place pertaining to the five Trust Factors: security, availability, processing, confidentiality, integrity, and privacy of customer data.

G Suite - Google protects the confidentiality and integrity of transmitted information by only accepting traffic that conforms to the specification of the network flow policy and by using reliable protocols with error correction to transmit information.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. There is a PRA collection for Ernest Hollings (0648-0568) and Dr. Nancy Foster scholarship (0648-0432)
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	X
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	X
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify): EBS communicates with NOAA staff prior to, during, and after all-hazards or emergency events. MS Dynamics – In order to support the management in accordance with Generally Accepted Accounting Principles (GAAP) of NOAA, trustee financial resources related to NRDA recoveries via settlement and Implementation of restoration projects conducted using these recoveries. AODocs – HR information is collected for the purpose of pay alignment, HR performance reporting, and HR management efforts. AODocs also collects BII for administering healthcare. BII that is specifically related to commercial contracts and financial information is collected for management, administration and information sharing. Only Virtru encrypted PII/PHI is stored in AODocs (Google Drive) to share sensitive personal and medical data securely in compliance with the Health Insurance Portability and Accountability Act (HIPAA). Customer related metadata is stored on Google App Engine DataStore which is FedRAMP approved, but not included under the NOAA Google ATO.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NOAA ENS is a cloud-based, software-as-a-service, vendor-hosted mass notification system that provides tools for reaching pre-defined contacts during an emergency situation. The purpose of the Emergency Notification System is to simplify management of emergency communication processes and procedures quickly and easily to communicate with all employees, Associates and visitors. This system is designed to help respond in a fast and decisive way during emergency situations. The multi-modal communications system, including phone, text, email, pagers, and more, allows NOAA to rapidly and efficiently reach our staff wherever they are. This ensures the life safety and security of all staff (including contractors) during emergencies.

The data collected contains personally identifiable information (PII) obtained from the NOAA Staff Directory (employees and contractors) and/or disclosed by the end-user for contacting in the case of emergency situations.

The encrypted PII/PHI collected for the medical library refers to federal employees (including NOAA Corps officers and U.S. Public Health Services (USPHS) officers). In some medical emergency instances, the reference may include contractors, members of the public, foreign nationals, and/or visitors. BII stored in AODocs libraries reference federal employees, contractors and commercial vendors.

For MS Dynamics, information on federal employees and contractors are included only to document expenditures based on their labor hours or contract level of effort.

Medical records on federal employees and contractors are imported into the AODocs library and protected using Virtru and Google Common Infrastructure. AODocs may contain Protected Health Information (PHI) or PII, such as full name, SSN, date of birth and email address.

G Suite collects email logs, authentication logs, basic user information, device information, calendar logs, and drive logs. The PII and BII stored and transmitted by G Suite are for the purpose of providing infrastructure and customer facing services to all NOAA staff.

MaaS360, Ivanti, Esri, Virtru and Smartsheet do not collect PII or BII.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example:

mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There is the potential threat that the privacy data being processed by users could be intentionally or unintentionally disclosed or shared with other unauthorized users. However, this risk is moderate because of the access, physical, and logical security controls that are in place to prevent this from happening. NOAA requires the use of CAC cards for physical and network access, and roles and privileges for application authorization. In addition, NOAA users that are involved in the handling or processing of the privacy data for the hosted applications are required to review and sign the Rules of behavior and take mandatory training in order to minimize such risks. The users are required to adhere to NOAA's policies regarding disclosure and separation of duties.

Although AODocs does not currently have a documented ATO, Virtru has been implemented to provide additional protection (revocation of access to shared documents). AODocs claims security inheritance from other assessed products, and claims "customer data stored in AODocs benefits from Google App Engine's security features, such as at rest encryption, the security of Google's network and the physical security of its datacenter facilities. Data storage in Google App Engine is highly redundant, with automatic replication across multiple datacenters." Google App Engine is a component of Google Cloud Platform, which is FedRAMP approved, but not included in NOAA's Google ATO.

<u>Section 6</u>: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	X
DOC bureaus	X		
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: EBS connects with NOAA0700 which contains the NOAA staff directory. There is no direct connection. The data is loaded onto a server and is downloaded by EBS. ESRI connects with NOAA0700, NOAA ICAM service for authentication. However, no PII/BII is sent or received between the systems. MSDynamics shares financial information with the NOAA MARS financial system. G Suite applications ensure email communications and file collaboration within NOAA. AODocs shares data using the AODocs interface in G Suite, and data managed by AODocs is split between data hosted on the G Suite environment of the Customer (through the intermediary of technical "storage accounts") and in the backend of AODocs, hosted on Google Cloud Platform. ServiceNow does not share data within NOAA, users access data via a secure website https://nsdesk.service-now.com/
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy for each application. The Privacy Act statement and/or privacy policy can be found at: https://www.homelandsecurity.noaa.gov/pdfs/PA-Statement-ENS.pdf https://www.homelandsecurity.noaa.gov/ https://www.everbridge.com/about/legal/privacy-notice/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-cloud-security-and-compliance-whitepaper.pdf https://www.servicenow.com/privacy-statement.html https://www.aodocs.com/terms-of-service https://privacy.microsoft.com/en-us/privacystatement	
	Yes, notice is provided by other	Specify how:

	means.	
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For EBS, work related PII is automatically uploaded to the system from the staff directory; However, personal PII, e.g. personal cell phone number, is optional. For AODocs, individuals may decline during the collection of PII/BII.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For EBS, users are presented with the options on the staff directory screen where data is optionally entered. The only uses for the information in the staff directory are for contacting staff routinely, or once the information is in EBS, for contacting staff by EBS in emergencies. In accordance with the Privacy Act Statement, for AODocs, the medical library is configured to allow individuals to consent or decline uses of their PII/PHI.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For EBS, users are presented with the option on the staff directory screen where data is optionally entered. This update reminder is displayed upon system entry for any purpose. For AODocs, based on document permissions, individuals may review and update PII/BII pertaining to them. Otherwise, individuals may contact the respective Library Administrator or AODocs System Administrator to update their PII/BII.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access is tracked through established access control/audit.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ___6/14/2019___ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks, other than those risks associated with AODocs application.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

For EBS, access is restricted, requiring authorized users, those with a "need to know" to log in. Account access is tracked. Information from the NOAA Staff Directory is uploaded to a server and downloaded by EBS, rather than having a direct connection.

G Suite, SmartSheet, and MaaS360 is encrypting based on FedRAMP requirements and adheres to the compliance standards of the Federal Information Processing Standard (FIPS). G Suite email and Drive has end-to-end encryption.

MS Dynamics uses Secure ICAM authentication with data at rest and based on FedRAMP requirements.

Virtru-enabled clients generate AES-256 bit symmetric encryption keys for each individual file. When encrypted, content is uploaded via AODocs, the creating Virtru client uploads Access Control Keys and policies to the Virtru Access Control Management via a Transport Layer Security (TLS) connection. The actual encrypted content rests in Google Drive, the storage platform for AODocs, which is FedRAMP certified. Customer metadata is stored on

Google App Engine, which is also FedRAMP certified.. The Virtru Zero Trust Architecture ensures separation of keys and content at all times.

From the Virtru dashboard, administrators control individual user privileges (decrypt-only or encrypt/decrypt). Users can also enable or revoke access to specific files they authored/created.

To encrypt and/or decrypt protected content, users must authenticate with their NOAA Google credentials. Users are required to verify their identity by using a Virtru verification code sent via email from verify@virtru.com.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: Yes, this system is covered by an existing system of records notice: *Department-1 Attendance, Leave, and Payroll Records of Employees and Certain Other Persons https://www.osec.doc.gov/opog/privacyact/sorns/dept-1.html **(AODocs)** *Department-2, Accounts Receivable https://www.osec.doc.gov/opog/privacyact/sorns/dept-2.html **(MsDynamics)** *Department-7, Employee Accident Reports https://www.osec.doc.gov/opog/privacyact/sorns/dept-7.html **(ServiceNow, AODocs, Everbridge)** Department-18, Employees Personnel Files Not Covered by Notices of Other Agencies, (http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html) **(Everbridge, AODocs)** *Department-25, Access Control and Identity Management System, http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html **(G-Suite)** *NOAA-22 NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSO). https://www.omao.noaa.gov/learn/marine-operations/about/project-planning/health-screening **(AODocs)** *OPM/GOVT-1, General Personnel Records, https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf **(AODocs, ServiceNow)** *OPM/GOVT-2, Employees Performance File Records https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-2-employee-performance-file-system-records.pdf **(AODocs)**

	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Requirements for record retention are found in the NOAA Records Schedules : 100-24 Information Technology Operations and Management Records and 100-27 Records of the Chief Information Officer, p.12 and the GRS 3.1, 3.2, 4.1, 4.2, 5.8, and 6.3.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	**Everbridge**: Individuals' name and mailing addresses are collected **ServiceNow**: Collects vehicle identification numbers when an accident occurs **AODocs**: This application is used to facilitate PHI and PII sharing.
X	Quantity of PII	PII is limited to contact information, Human Resources information, and some limited medical administrative information. As this information is collected across NOAA for multiple usage, the amount of information contained within this boundary is noted and will be larger than usual.
X	Data Field Sensitivity	**AODocs**: Sensitive PII is transmitted **MSDynamics**: Sensitive BII is stored/transmitted to this application.
X	Context of Use	Cloud applications residing in the NOAA0900 boundary are used for a variety of critical business processes that require the storing/transmission of PII/BII.
X	Obligation to Protect Confidentiality	NOAA has the obligation to protect personal information collected in routine Human Resources operations. Additionally, some limited medical administrative data is collected (flight status). NOAA is obligated to protect this information. The Privacy Act of 1974 requires us to safeguard the collection, access, use, dissemination and storage of BII and PII.
X	Access to and Location of PII	Access to each component application is managed through the respective application's access in that application's CSP. The location of the information resides within each CSP virtual environment.
	Other:	Provide explanation:

<u>Section 12</u>: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There is the potential threat that the privacy data being processed by users could be intentionally or unintentionally disclosed or shared with other unauthorized users. However, this risk is low because of the access, physical and logical security controls that are in place to prevent this from happening. NOAA requires the use of CAC cards for physical and network access, and roles and privileges for application authorization. In addition, NOAA users that are involved in the handling or processing of the privacy data for the hosted applications are required to review and sign the Rules of Behavior and take mandatory training annually (or as needed) in order to minimize such risks. The users are required to adhere to NOAA's policies regarding disclosure and separation of duties.

AODocs is NOAA approved. AODocs claims security inheritance from other assessed products, and states "customer data stored in AODocs benefits from Google App Engine's security features, such as at rest encryption, the security of Google's network and the physical security of its datacenter facilities. Data storage in Google App Engine is highly redundant, with automatic replication across multiple datacenters." Google Cloud Platform has NOT been given a NOAA ATO. Additionally, Virtru has been implemented to provide additional protection for AODocs. AODocs relies on Virtru to comply with federal data privacy policies, laws and regulations.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.