Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA0900, Consolidated Cloud Applications

U.S. Department of Commerce Privacy Threshold Analysis

NOAA0900/Consolidated Cloud Applications

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

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).

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
Mass 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 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, 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 information: 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 Google Cloud Platform (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 does not collect PII or BII.

MaaS 360: MaaS360, a SaaS provider, 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) as well as desktop and laptop management to customers.

MaaS360 embodies the following five essential cloud characteristics defined by NIST Special Publication (SP) 800-145 "The NIST Definition of Cloud Computing":

- On-demand self-service environment,
- Broad network access is supported,
- Resource pooling and multi-tenancy is core to the design,
- Capabilities can be rapidly and elastically provisioned, and
- Measured service principles are implemented with resources automatically controlled and optimized.

The cloud computing service delivery model MaaS360 is SaaS model. In this delivery model, IBM is responsible for all of the service delivery layers including; infrastructure (i.e., hardware and software that comprise the cloud infrastructure); data security, and service management processes (i.e., the operation and management of the infrastructure and the system and software engineering lifecycles). Federal agencies are responsible for managing the customer configurable options, for authorizing, granting and reviewing administrator access and for reviewing logged activity.

MaaS360 is a system that customers can use to monitor and control the security posture of their desktop and laptop computers and also of other items in their mobile device inventory, such as smart phones and tablet devices. For MaaS360 to monitor and control devices, each managed device needs to be registered with MaaS360 and then must periodically connect to MaaS360 both in order to update MaaS360 with current device status and with any relevant events and also to receive security configuration updates from MaaS360. Although at a basic level, this service delivery concept is the same for all managed devices, the mechanisms used vary for different types of devices.

IBM customers use the MaaS360 Portal, a cloud-based management console, to manage the security of desktop and laptop computers and other mobile devices such as smart phones and tablet devices. For each customer organization, at least one user is given administrator access to configure, monitor, and manage the organization's implementation of MaaS360 using the MaaS360 Portal.

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

Service Now: ServiceNow, a SaaS provider, is an application hosted at Terremark facilities in Manassas, VA and Miami, FL. It is an appliance-based solution for remote support to desktops, laptops, and other approved devices.

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. ServiceNow applications cover all Information Technology Infrastructure Library (ITIL) processes and are natively integrated on a single platform providing web intuitiveness an unprecedented process automation.

ServiceNow is a modular solution, meaning that customers may use all, or a sub-set of the applications provided via ServiceNow. Additionally, these applications may be implemented in a modular fashion.

A ServiceNow SaaS application is a group of modules, or pages, that provide related information and functionality in a ServiceNow instance. For example, the Incident application contains modules for creating and viewing incidents; the Configuration application contains modules for configuring servers, databases, and networks. The Application Navigator (or left-navigation bar) within the ServiceNow user interface, provides links to all applications and the modules they comprise enabling users to quickly find information and services. Administrators can customize the Application Navigator to provide different modules by user role, modify or define applications and modules, and change its appearance. These SaaS applications can be added or removed by enabling or disabling the application‘s Plugin.

The ServiceNow Service Automation Government Cloud Suite is physically and logically separated from the ServiceNow Public Cloud offering. The ServiceNow Service Automation Government Cloud Suite is hosted in two dedicated data center cages that house infrastructure dedicated to the Government Community Cloud. Logically, ServiceNow‘s network architecture and access controls separate the ServiceNow Government Community Cloud from the ServiceNow Public Cloud. ServiceNow single-tenant environment ads an additional layer of logical separation for instances.

Federal customers share a hardware platform (no virtualization), but access entirely separate individual instances of the ServiceNow platform located in the dedicated federal data center cages. Each individual instance connects to a database only accessible by that specific instance.

The ServiceNow Service Automation Government Cloud Suite consists of the out-of-the-box applications in addition to the ServiceNow Discovery Application and ServiceNow Orchestration (Orchestration) Application. The ServiceNow Discovery Application and ServiceNow Orchestration (Orchestration) Application are sold separately from the ServiceNow out-of-thebox applications. The ServiceNow Discovery Application and ServiceNow Orchestration

Application are not required for the system to operate or relied on for security control implementation. Thus, if not purchased the system security is not negatively impacted. All applications in the table below are general applications part of the ServiceNow Service Automation Government Cloud Suite within the testing scope of the FedRAMP authorization.

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.

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 are 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 Divison) to provide and monitor help desk support and manage internal FSD configuration and management requests.

The authorization boundary of the Ivanti Service Manager (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 datacenter 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, customer 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 another information system 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 distribute Standard Operating Procedures, manage quality control processes, and assist in the coordination of contract management, procurements, intranet publication and incident reporting. AODocs is not FedRAMP certified but does rely on Google infrastructure to deliver its product (G Suite) and backend (Google Cloud Platform), which is FedRAMP certified. AODocs is the subject of a PL-2 POA&M which requires a full NOAA ATO evolution be conducted on the application.

AODocs, has not been vetted through the Authorization to Operate (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.

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 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).

Dynamics 365 for Government inherits several client-optional interconnections with other Microsoft services (Yammer, Exchange Online, SharePoint Online, other POP3 / IMAP services) from the commercial public cloud, multi-tenant deployment of Dynamics 365. In order to ensure the Dynamics 365 for Government system can maintain an appropriate security posture, these interconnections have been disabled by default within the production environment. Although the functionality is still present, Dynamics 365 for Government presents a disclaimer when a customer user attempts to access the functionality, to ensure appropriate disclosure that these services are not within the Dynamics 365 accreditation boundary. These client-optional interconnections can only be enabled by customer administrators.

Dynamics 365 is a multi-tenant architecture made up of traditional web application and SQL database servers deployed across two Azure for Gov. datacenters for business continuity. Logically the architecture in each datacenter comprises of site wide roles that provides routing capabilities within a datacenter POD and Scalegroup. A POD consists of 16 scale groups and shared resources that provide reporting and sandbox plugin capabilities across all the scale groups. Each Scale group is designed to include shared resources such as web servers and async

servers (job servers) with redundancy across all server roles for high availability. Every scale group also includes private resources such as dedicated primary tenant SQL databases and secondary databases for data isolation that means every customer gets their own dedicated database and URL.

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.

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, email, and a biography. 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 diagram below visualizes the Virtru encryption process. The Virtru client application uses a secret key (Access Control Key/Key V) 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 (Payload Key/ Key P) via TDF. A separate key, known as a Split Knowledge Key (Key M), 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 Diffe-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. Customer 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 collects medical records that will include information such as full name, social security number, date of birth, and email address.

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

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.

b) System location:

Silver Spring MD.

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	FedRAMP ATO	MODERATE
G-Suite	FedRAMP ATO	MODERATE
Maas 360	FedRAMP ATO	MODERATE
ServiceNow	FedRAMP/NOAA ATO	HIGH in process/MODERATE
SmartSheet	FedRAMP ATO	MODERATE

Ivanti	NOAA approved, FedRAMP Ready	MODERATE
AODocs	NOAA Approved/FedRAMP Moderate in Process	FedRAMP Moderate in Process
MS Dynamics	DOC approved ATO	HIGH
ESRI	FedRAMP (Dept of Interior approved) ATP	Low
Virtru	FedRAMP Moderate 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 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, use, or disseminated by the system:

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

G-suite collects email logs, authentication logs, basic user information, device information, calendar logs, and drive logs. G-suite does not collect PII or BII.

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.

Smartsheet does not collect PII or BII.

Ivanti does not collect BII or PII.

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.

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.

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

Virtru collects medical records that will include information such as full name, social security number, date of birth, and email address.

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. EBS is implemented in compliance with FedRAMP requirements (FIPs 140-2 validated encryption).

EBS - Information is uploaded from the NOAA Staff Directory and alerts are sent out to NOAA staff and contractors by the system.

G-suite – Google e-mail and Google Drive has end-to-end encryption.

MaaS360 does collect PII or BII.

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

Smartsheet uses Transport Layer Security (TLS) technology to encrypt all data transmission.

Ivanti does not collect PII and BII.

AODocs - Information is transmitted to AODocs via the manual upload button in the web browser. Files are also uploaded to AODocs via email or import from Google Drive. Information is downloadable from the AODocs web interface or from Google Drive. Google Drive uses end-to-end encryption.

MS Dynamics – All traffic is via restricted secured zone under Microsoft 365 GCC (NOAA SDD tenant space). All data is encrypted.

Esri – All traffic to and from the NOAA GeoPlatform (ArcGIS Online) is via HTTPS secure web requests.

Virtru - Information is transmitted to and from Virtru exclusively via the AODocs interface. Virtru-encrypted files are only decrypted by being redirected to the Virtru Secure Reader.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

_X__ 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	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 contain PII and BII: EBS, G-suite. MaaS360, SmartSheet, Ivanti, AODocs, MsDyanamics, Esri, 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. *Continue to answer questions and complete certification.*

____ 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). *Skip questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later). *Skip questions and complete certification.*

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.

____ Yes. *Please describe the activities which may raise privacy concerns.*

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

__X__ 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 personally identifiable information 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
____ National Institute of Standards and Technology Associates

_X___ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

__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 and protected using Virtru. Virtru contains 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: ● FDIC Privacy Act SORN 30-64-0033 ● https://www.fdic.gov/regulations/laws/rules/2000-4000.html#fdic200030--64--0033 ● Department-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, ● Department-13, Investigative and Security Records, (http://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/commerce-department-13.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) ● GSA./GOVT-7, Personal Identity Verification Identity Management System, (http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570728/gsagovt-7/) ● NOAA-14, Dr. Nancy Foster Scholarship Program, which has been revised to include Ernest F. Hollings Undergraduate Scholarship Program and the National Marine

Fisheries Service Recruitment, Training, and Research Program alumni survey. Also,

- 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 would cover the personnel related records created and maintained by Supervisors, and WFMO, both those that go in the eOPF, and those held by the chain of command. (https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-2-employee-performance-file-system-records.pdf)

____ 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, 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 NOAA 0900 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): Stefan Leeb

Signature of ISSO or SO: LEEB.STEFAN.ANTON.1158781260 2020.03.27 17:58:54 -04'00' Date: 3/27/2020

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: OBENSCHAIN.CHARLES.THOMAS.1506347293 Digitally signed by OBENSCHAIN.CHARLES.THOMAS.1506347293 Date: 2020.03.30 15:37:16 -04'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2020.03.30 16:38:57 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.03.31 07:05:43 -04'00' Date: _____