Information	
The following checklist represents GovRAMP's requirements for the Authorization Boundary Diagram (ABD) and should be used by Service Providers when developing the ABD	
GovRAMP Document	**Reviewed Requirements Are Depicted or Diagram Uploaded** **Choose: Yes, No, N/A?**
ABD Checklist	
ABD is an easy-to-read diagram with a clear legend. If necessary to achieve a high enough resolution, attach diagrams separately.	
A prominent, contiguous **RED** border is drawn around all components in the authorization boundary.	
All ingress and egress points are depicted.	
All IaaS regions and zones are depicted.	
All virtual private clouds (VPCs) are depicted.	
All subnets are depicted.	
Application plane is depicted.	
Management plane is depicted.	
All services leveraged from underlying IaaS and/or PaaS are depicted.	
All services leveraged from SaaS are depicted.	
All services that are NOT GovRAMP authorized are clearly identified.	
All interconnected systems are depicted.	
All external services, including corporate services, are depicted.	

Every tool, service, or component mentioned in the SSP narrative is depicted. This includes services provided by the system and internal tools used to manage the system. These tools can be inside the boundary or outside the boundary.	
How SP users access the cloud service (including authentication method) is depicted.	
How SP admins access the cloud service (including authentication method) is depicted.	
How SLED customers access the cloud service (including authentication method) is depicted.	
Components provided by the SP and installed on customer devices are depicted inside the authorization boundary (if applicable).	
Customer-side, on-prem components provided by the SP are depicted. If in scope for 3PAO testing, these components should have a separate red border around them while still being depicted in the customer environment.	
Connections between components within the boundary are shown.	
Connections to/from external services are shown.	
Separation and security controls between the boundary and external services are depicted.	
Separation and security controls for access into the boundary are depicted.	
Dev/test environment is depicted (if applicable) with connections to the production environment. Security mechanisms for the connections should be depicted.	
Alternate processing site is depicted (if applicable). Alternate IaaS zones/regions should be depicted if leveraged as an alternate processing site. Connections to the production environment and security mechanisms for the connections should be depicted.	
Location where backups are stored is depicted along with connections to the backup storage location. Security mechanisms for the connections should be depicted.	
Dev/test environment is included within the boundary if SLED data is used.	
Dev/test environment is included within the boundary if SLED personnel have any access (including training or UAT).	
Update services (e.g., malware signatures, Operating Systems, software) are depicted outside the boundary with connections shown to the production or dev/test environments.	
Each service leveraged from the underlying IaaS/PaaS should be clearly depicted in a separate legend.	
APIs used by the product. Security mehcanisms should be depicted.	

Corporate shared services.	
Customer IdP used for authentication is depicted as out-of-boundary (if applicable).	
2.5.2 Network Diagram Checklist	
Network Diagram includes all components reflected in the ABD.	
Subnetting is clearly depicted. Subnets should be labeled by function.	
Location of DNS servers is depicted. Data flows should be depicted to show how DNS functions in the system.	
External authoritative DNS servers used by customers to access the CSO are depicted.	
Internal recursive DNS servers used to access domains outside the boundary are depicted.	
2.5.3 Data Flow Diagrams (DFDs) Checklist	
DFDs include all components reflected in the ABD.	
SLED customer user authentication flow is depicted, including type of MFA.	
SLED customer admin authentication flow is depicted, including type of MFA.	
SP administrative personnel authentication flow is depicted, including type of MFA.	
SP support personnel authentication flow is depicted, including type of MFA.	
System application data flow within the Authorization Boundary is depicted, including encryption for all flows.	
System application data flow to/from external services is depicted, including encryption for all flows.	
Data flow to/from corporate shared services is depicted, including encryption for all flows.	
Data flow to/from interconnected systems is depicted, including encryption for all flows.	
Data flow to/from alternate processing sites is depicted, including encryption for all flows.	
Data flow to/from backup storage is depicted, including encryption for all flows.	
Data flow to/from dev/test environment is depicted, including encryption for all flows.	
If necessary, the DFD may be separated into separate diagrams for each type of data flow. For each of these separate DFDs, explicitly identify:	

Every location (internal & external) where SLED data at rest is NOT protected through encryption.	
Every location (internal & external) where SLED data in transit is NOT protected through encryption.	
Every location where SLED data at rest IS protected through encryption.	
Every location where SLED data in transit IS protected through encryption.	

The solid black line is used to show data or communication that either enters into or exits from the "Company name" Commercial Authorization Boundary. Any other traffic lines are strictly controlled with additional steps like MFA, OTP, or YubiKey

Any icon name or depicted is for reference only and is not the only style or type of icon that may be used. VISIO has limited icons available for some icons. The most important part is that the CSP articulates the products, ports, protocols and services within the authorization boundary. This is provided for illustrative purposes only and does not constitute an endorsement of any products mentioned.

Legend

- Authorization Boundary
- Product Commercial Boundary
- Region
- Product Services Instances
- Product Servies
- VNET
- Subnet
- External Services
- Shared Corp Services
- DNSSEC
- User Access Federated
- User Access Non-Federated
- Mobile App
- IT Admin Access
- Admin Portal Access
- "Company" Admin Access
- Update Sources
- Software Deployment (pull)
- Software Deployment (push)
- Logging
- Backups
- Notifications
- Monitoring
- Livetest Dev/Test
- Internal API
- External API
- Internal DNS
- NTP
- SQL Traffic
- SQL Traffic NP

Type or Series of MFA: MFA ICON FIPS Series FIDO2, WEBAUTHN

Data in Storage Full Disk | Data in Storage FIPS

INFORMATION
All internal traffic, incoming and outgoing calls utilize HTTPS 443 FIPS 140-2 TLS 1.2 unless otherwise noted.

"Product" Services are replicated within "Company Name" Authorization Boundary as traffic would ingress through "Product" Commercial Cloud API Gateway before entering "Company Name" API Gateway to utilize "Product" Services Instances within "Company Name" Authorization Boundary

"DATA CENTER" South Central serves as the recovery site for "Company". "Product Name" has pre-built all the VLANs, subnets, Active Directory controllers, SQL servers, and other network infrastructure to facilitate rapid recovery. Under normal operations, no "Company Name" traffic exist in South Central Region except for SQL replication, Active Directory replication, and NTP. In the event of fail-over, all other virtual machines would be restored from "DATA CENTER" Site Recovery and traffic in South Central would appear similar to that of North Central.

Customer Premise

No CSP-managed software is deployed within the customer's premise.

"Product Name" (e.g. AWS, Azure, etc.): (FedRAMP Authorized, Package ID: FXXXXXXXXX) (GovRAMP Authorized, Package ID: SRXXXXXX)

AWS/Azure/Google Product Services

"Product" WAF Icon | NAT Gateway | NAT Gateway | Web Apps (App Service) | Recovery Services Vaults | Application Gateways | Update Manager

Portal Icon | "Product" Load Balancer Icon | Availability Sets | DataBase | Storage Accounts

External Services

Not FedRAMP Authorized: Product Name | Product Name | Product Name | CodeBuild | DevOps

GovRAMP / FedRAMP Authorized: Product Name Package ID: GovRAMP/FedRAMP | Icon / Product Name Package ID: GovRAMP/FedRAMP | Product Name Package ID: GovRAMP/FedRAMP

Federated SAML 2.0 IDP | Confirm User Identity | Verify User SAML 2/CAC/PIV | Identity Store | HTTP/HTTPS 443 | SAML Request | HTTPS 443 TLS 1.2 FIPS Authentication Flow

Shared Corp Services: Training Repository | OS Image Icon | Active Directory Cloud | Active Directory Onsite | Code testing LOGO HERE | LOGO HERE | LOGO HERE

CSP Administrators: MFA ICON "Main" Developers QA Analysts | MFA ICON "Main" admin | IT Admin MFA ICON

Clients: User Non-Federated | User Federated | User "Company" Mobile App | User Client

Product Icon or LOGO | LIST Product URLs | Request | Resolve | DNSSEC 53

Internet | SMTP 587 FIPS 140-2 TLS 1.2

Update Sources: Tool Icon | OS Image Icon | Tool Icon | SIEM Tool Icon | HTTP/HTTPS 443 Signature Updates

US North Central Region (Primary Site)

Authorization Boundary

NAT "System Name" Public IP Address "System Name" IP Address "System Name" IP Address | IP Icon | Applications would be making a pull request.

HTTPS MailGun | SMTP 587 Mailgun | TCP port tbd with ESSDS

Virtual Networks "System Name" | Network Security Groups "System Name" "System Name"

"Subnet Name" IP Address: Application Gateway "System Name" IP Address Public IP Address "System Name" IP Address

Resource Group- "NAME"- Production VNET- "NAME- IP Address"; DNS- "Address"

"Subnet Name" IP Address: App Service Plan "System Name" | Function App "System Name" "System Name" | Service Bus Namespace "System Name" | Storage Account "System Name"

"Subnet Name" IP Address: App Service Plan "System Name" | Function App "System Name" "System Name" | Service Bus Namespace "System Name" | Storage Account "System Name" "System Name"

"Subnet Name" IP Address: App Service Plan "System Name" | Service Bus Namespace "System Name" | Storage Account "System Name" "System Name"

"Subnet Name" IP Address: Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address

"Subnet Name" IP Address: App Services/WWW "System Name" "System Name" | App Services (Slot) "System Name" "System Name" | App Services (Slot) "System Name" "System Name" | Function App "System Name" "System Name" | App Service Plans "System Name"

"Subnet Name" IP Address: Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address

Flow Log "System Name" "System Name" | Availability Sets "System Name" | Availability Sets "System Name" | Availability Sets "System Name" | Availability Sets "System Name" | Storage Account "System Name" "System Name" "System Name" "System Name" "System Name" "System Name"

"Subnet Name" IP Address: Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address

"Subnet Name" IP Address: Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address

"Subnet Name" IP Address: Private Endpoint "System Name" IP Address | OpenAI "System Name" IP Address | Private Endpoint "System Name" IP Address | AI Document Intelligence "System Name" IP Address | Resource Group "System Name" IP Address | Managed Identity "System Name" IP Address | Private DNS Zone "System Name" IP Address | Private DNS Zone "System Name" IP Address

"Subnet Name" IP Address: Load Balancers "System Name" IP Address | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address | Storage Accounts "System Name" "System Name" "System Name" | SQL Server "System Name" | SQL Elastic Pools "System Name" | DataFlow1 Data School | Data in Storage FIPS | All VM/ Internal DNSSEC UDP 53 to Active Directory servers

"Subnet Name" IP Address: ACI - Container Instances "System Name" IP Address

"Subnet Name" IP Address: Private DNS "DNS System Name" "DNS System Name" "DNS System Name"

"Subnet Name" IP Address: Managed Identity "System Name" "System Name" | Storage Account "System Name" | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address

"Subnet Name" IP Address: Virtual Machine "System Name" IP Address

SMTP 587 FIPS 140-2 TLS 1.2 | HTTP/HTTPS 443 Signature Updates

Resource Group- "NAME"- Management VNET- "NAME"- IP Address

"Subnet Name" IP Address: Virtual Network "System Name" IP Address DNS IP Address | Bastion "System Name" | Network Security Group "System Name" | Public IP Address "System Name" IP Address

"Subnet Name" IP Address: Network Security Group "System Name" | Container Instances "System Name" IP Address | Container Registry "System Name" | Container Registry replication "System Name" "System Name" | RDP 3389 with FIPS 140-2 Authc Password Internal AD

"Subnet Name" IP Address: Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address | Virtual Machine "System Name" IP Address

App Service Plans "System Name" | Restore Point Collection "System Name" | Function App "System Name" | Storage Account "System Name" "System Name" "System Name" "System Name" "System Name" | Network Watcher "System Name" "System Name" "System Name" "System Name" | Solution "System Name"

Private DNS "DNS System Name" "DNS System Name" "DNS System Name"

Front Door and CDN profile "System Name" | Web Application Firewall Policies "System Name" | "Subnet Name" | HTTPS with FIPS 140-2 TLS1.2 Auth: Password + DUO MFA push

Google/AWS/Azure Product Services Instance: Portal Icon | Key Vault Icon "System Name" | Product Function Applications Icon | Log Analytics Workspaces | Application Insights

"Product" Services are replicated within "Company Name" Authorization Boundary as traffic would ingress through "Product" Commercial Cloud API Gateway before entering "Company Name" API Gateway to utilize "Product" Services Instances within "Company Name" Authorization Boundary

US South Central Region (Alternate Site)

NAT Gateway "System Name" Public IP Addresses "System Name" IP Address "System Name" IP Address

Virtual Networks "System Name" IP Address | Network Security Groups "System Name" "System Name"

"Subnet Name" IP Address: Application Gateways "System Name" IP Address "IP Address" equipleway Public IP Addresses "System Name" IP Address | Automation Account "System Name" | Storage Accounts "System Name" "System Name" "System Name" "System Name" "System Name" "System Name"

"Subnet Name" IP Address: Availability Sets "System Name" | Availability Sets "System Name" | Availability Sets "System Name"

Resource Group- "NAME"- Production VNET- "NAME"- IP Address

"Subnet Name" IP Address: Load Balancer "System Name" IP Address | Virtual Machine "System Name" IP Address | SQL elastic pool "System Name" | SQL Server "System Name" | Storage Account "System Name"

"Subnet Name" IP Address: Function App "System Name" "System Name" | App Services (Slot) "System Name" "System Name" "System Name" "System Name" | App Service "System Name" "System Name" | App Service Plan "System Name" | Restore Point Collection "System Name"

"Subnet Name" IP Address | "Subnet Name" IP Address | "Subnet Name" IP Address: Container Instances "System Name" IP Address | "Subnet Name" IP Address: Virtual Machine "System Name" IP Address | "Subnet Name" IP Address | "Subnet Name" IP Address

Private DNS "DNS System Name" "DNS System Name" "DNS System Name"

Resource Group "NAME"-Management VNET-"NAME"-IP Address

Virtual network "System Name" IP Address DNS IP Address

"Subnet Name" IP Address: Network security group "System Name" | Bastion "System Name" | Public IP Address "System Name" IP Address

"Subnet Name" IP Address

Private DNS Zone "DNS System Name" | All VMs backed up nightly

Azure/AWS/Google Services Instances: Backup | Replication Icon "System Name" | Replication Services Production | Replication Services Management | Replication Services LiveTest | Replication Services GoldTest

At times there are two functions happening (e.g. Storage and Replication)

Azure Function | User Jacome Function | "System Name" (Geo-Replicated)

"DATACENTER NAME" North Central Data Replication Paths

"System Name" | Initial Vault "System Name" | Replicated Vault: "System Name"

INFORMATION
The dashes here are only meant to help distinguish the data flows from Azure North Central Server Names to the correlated Initial ASR Vault then onto the Replicated ASR Vault within Azure South Central Region.

"DATACENTER NAME" South Central Data Replication Paths

"System Name" | Initial Vault "System Name" | Replicated Vault: "System Name"