MSISR Frequently Asked Questions

Please email msisrops@microsoft.com for any questions not answered in the sections below.

Availability

Are availability sets available in MSISR?

Availability Sets are available, availability Zones are NOT. VM Scale Sets are available as well.

Authorization

Is there a design diagram with auth boundaries?

Please see the authorization design doc

What is the UID of the Information System (i.e. package number in eMASS)?

There is not a DCSA or Authorizing Authority Specific eMASS package for MS-ISR. This is approved under a DISA PA. Each DIB partner will submit an ATO package to DCSA or Authorizing Authority in eMASS for their instantiation of their Data and Mission Planes. This will be a unique by-DIB ATO from DCSA or Authorizing Authority. More information about DISA eMASS IDs can be found on the Authorization wiki page.

Who is the Authorizing Official for an MS-ISR Instance?

Microsoft is responsible for maintaining the PA with DISA for MS-ISR and administering the Control Plane.

The Partner is responsible for the ATO of their Data and Mission Plane. It is recommended that the Partner achieve one ATO to cover the framework of the Data and Mission Planes, allowing multiple Mission Workloads to be onboarded into the Mission Plane without additional ATOs.

- For the DIB, ATOs for the Data and Mission Planes will be issued by DCSA.
- For non-DIB partners, ATOs for the Data and Mission Planes will be issued by DISA or under an MOA between DISA and an OGA.

What are the names of the DCSA Regional Authorization Official (RAO) and NISPOM AO (NAO)?

The AO who approves DiB Partner's is the DCSA East United States AO, Alex Hubert. The location of the DIB partner's system will dictate which AO is assigned by DCSA.

What architecture/connectivity pattern has been approved by DCSA or Authorizing Authorities so far?

DCSA has authorized a thin client-based architecture where a DIB customer procures thin clients, creates a WAN, and connects them to Azure Secret to utilize MS-ISR. DCSA will also authorize a Thick Client at each on-premises site for use as Data Transfer Station and for out-of-band administrative access.

In addition, DCSA will also allow, after review and approval, an Interconnection Security Agreement (ISA) between the DCSA authorization boundary and external on-premises networks. Once in place on-premises systems can communicate bi-directionally with in cloud systems according to the security and network rules allowed by DCSA and implemented by Partner Data Plane administration team.

Does MS-ISR support hybrid connectivity to on-premises systems?

MS-ISR and Azure Secret are able to support hybrid connectivity to on-premises systems. Requests for hybrid connectivity to on-premises systems will need to be worked by each DIB with DCSA or Authorizing Authority with their specific requirements. DCSA or Authorizing Authority is the approval authority.

Collaboration

What is the current status of O365 for the DIB?

Currently O365 Secret is only available to government and DoD customers. There is intent to make it available to DIB partners, but we don't have an estimated date. Microsoft is working with DISA for this approval.

Is the partner responsible for licensing the Exchange/Sharepoint/Skype components of the collaboration suite in MS-ISR?

Yes, the partner is responsible for procuring the required Office server licensing. This can vary by partner, and they should work with their own internal Licensing team on the best way to approach the procurement. If they need further assistance, we can refer them to the Microsoft AE or CSAM for more assistance.

Can the collaboration suite be added at a later date, after the initial tenant deployment?

Yes, they can be added at any point through a request to the MS-ISR team or the customer can deploy their own collab tools from scratch as well.

Connectivity

Does the National Security Terms and Conditions (T&Cs) hold prevent a partner from deploying network gear (once procured) to the Microsoft data center?

Microsoft needs a DD254 as well as an authorization from DCSA or Authorizing Authority stating that the system is approved to connect (ATC). Once the approval is received we will work with you to arrange for equipment setup.

Does the /16 requested for MS-ISR (as noted in the MS-ISR On-Boarding guide) need to be SIPR-Routable IP Space?

No - this IP space does not need to be requested from the Government's allocation, but should not conflict with the current on-prem IP allocations to prepare for/enable hybrid connectivity between on-prem systems and your Azure Secret environment.

Are there transit networks in the Data plane that vnets in the mission plane connect to or are vnets shared between Data and Mission planes?

Mission planes are provisioned a spoke vNet that is peered with the data plane. Supporting services can be reached through this.

What are the IP/Subnet requirements for Hybrid Connectivity Scenarios including Commercial-as-Transport options?

All hybrid connectivity scenarios require **ER Direct** for **Red Side** connectivity once customer has extended their network to the Azure Secret Datacenter either by bringing their own circuit or leveraging the commercial-as-transport SCP ER provider. The Microsoft Peering config for circuits using the ER Direct must use DoD IP space that has been allocated by the DoD NIC. The Private Peering config for circuits using the ER direct will use partner provided private IP address space that is deconflicted with any on-premises ranges.

In commercial-as-transport SCP provider scenarios the unclassified IP space between public and USSEC will be allocated by partner and live in the private peering/private VNET routing domain and will need to align with schema used for unclassified transport network. Also, the black side SCP provider handoff to partner router/crypto device will be 2 x interfaces split across a switch pair and partner should allocate a subnet to each. There are 2 choices to advertise those routes, either MSFT will advertise the subnets to BGP as connected networks or partner can BGP peer to SCP.

Is DIB SIPRNET access needed to standup the IL6 MS-ISR environment?

No. The MS-ISR solution is specifically designed to restrict DIB users from accessing SIPRNET from this environment. One of the items DISA has required of MSFT for this solution is to ensure there is no SIPRNET-backflow from the MS-ISR Azure environment into other government networks such as SIPRNET. This is one of MSFT's primary duties in the Control Plane. While Azure Secret is connected to SIPRNET, MS-ISR DIB tenants will not be allowed by MSFT Control Plane policies to route to SIPRNET or SIPRNET resources. Instead, the DIB partner will need to establish a connection to Azure Secret (there are multiple options to accomplish this) and work from that DIB-connected system.

If we are ok foregoing the possibility of future hybrid connectivity to IL4, are we OK to use an overlapping space?

Yes, but it is highly advisable to future-proof the network design and pre-onboarding is the correct time to deconflict this.

If we receive two 10Gbps handoffs on the Red side into our Layer3 switch I assume we will have (2) BGP peers (1) off each link?

Yes

Does partner assign private IP ranges for the links between Red switch and Azure and if so are these both /30s?

A pair of private /30 subnets that aren't part of any address space reserved for virtual networks. One subnet is used for the primary link, while the other will be used for the secondary link. From each of these subnets, you assign the first usable IP address to your router as Microsoft uses the second usable IP for its router.

How do you handle BGP ASN assignments, should we be using private or public ASNs?

You can use both 2-byte and 4-byte AS numbers. You can use a private AS number for this peering except for the number from 65515 to 65520, inclusively.

Do you support and or are we looking to perform BGP Authentication or BFD for fast convergence?

We do support BFD over Express Route, https://learn.microsoft.com/en-us/azure/expressroute/expressroute-bfd . That design decision is up to you, not required by us.

Besides the public routes are we assigning all the private IP addressing on the Azure Cloud service side?

Yes

Do we need to enable standard or extended communities for anything?

There are no requirements for communities.

Is the low/black side shared space or separate in nature, data halls, cages, controls?

The black side hardware will be placed in a shared locked unclassified rack, but still within the classified/accredited physical security boundary/data hall.

What are the Red Rack Dimensions and Configuration?

14U locked compartment minus 2U for A/B PDU's = 12U usable red rack space dedicated to Partner

Can partner bring laptop/configuration device into the MS DC to finish configurations or will some onsite workstation be provided by MS?

Yes. The data center will require you to attest that you have run a virus scan within 24 hours of your visit.

Do partner personnel require a specific clearance level to enter the datacenter?

Yes, TS

Will Microsoft provide patch cables?

MSFT will provide SM patch cables between customer hardware and the patch panel terminating the SM structured cable plant. Connector type = LC

Single Mode Fiber Used?

Yes

Length to MS low side transport?

Must patch to SM cable plant between red and black rack

Length to high side rack?

Must patch to SM cable plant between customer red rack and ExpressRoute red rack

If copper within red rack does it require "shielded"?

Yes

Will partner have network capability and or Phone service around the secure space?

There is no unclassified communication service in the secure space.

Are we doing Dot1Q both Black and Red MS handoffs? If so is MS assigning these VLANs or us?

Dot1Q is only required on the Red side. These can be any VLAN that you assign. You will coordinate with MS-ISR Team who will be provisioning the ExpressRoute circuits/peerings. On the Black side there is no plan to use Dot1Q.

For the racks that house the Black and Red equipment, who controls the keys and or has keys?

Keys for racks are secured in a TRAKKA key system. Only Microsoft personnel have access to the keys. For Red keys customers can check out their key. For Black, since it is shared rack space, only Microsoft can control the keys, in which case all customer access is escorted.

Cost Management

How much does MS-ISR cost to Run?

See Consumption Costs for base cost information.

Development

We typically deploy pre-prod and prod in Azure and ASH using different vnets to separate the two, would there be any restrictions to this approach or limitations in the number of vnets deployed?

The same restrictions to resource limits apply per subscription. Mission Planes are subscription based so you could either separate by Mission Plane and vNet or use just vNets within a single Mission Plane.

Data Security

What should a Partner do if there is a Data Spill outside of their MS-ISR Tenant?

If there is a concern where the spillage is believed to have been leaked out of the MS-ISR tenant into Azure Secret somehow, the Partner would contact the MSFT NST (FSO@microsoft.com), who in turn would contact the cyber/soc team for Azure Secret for data spillage procedures.

How can partners secure access to storage accounts?

Azure offers a few ways to secure access to storage accounts. When a storage account is created, Azure generates 512-bit storage access keys, which, when combined with the storage account name, can be used to access the data objects stored in the storage account. Access to these storage access keys can be controlled using Azure Active Directory Role-Based Access Control (RBAC), ensuring that users have only the access and permissions they need. Additionally, Shared Access Signatures can be used to secure access to specific data objects stored in a storage account (e.g., blobs, files, queues, tables).

Can partners encrypt storage?

Yes, Azure customers can encrypt storage in several different ways. Azure Storage Service Encryption (SSE) provides 256-bit AES encryption at rest for Azure Storage accounts, transparently handling encryption, decryption, and key management. SSE is enabled by default for all storage accounts and any blobs written to the storage account will be encrypted.

Does Microsoft have access to data in partner's storage accounts or encryption keys?

You own your data. Microsoft uses customer data only to provide the services we have agreed upon, and for purposes that are compatible with providing those services. Access to customer data by Microsoft employees is restricted based on business need by role-based access control, multifactor authentication, minimizing standing access to production data, and other controls. Access to customer data is also strictly logged, and both Microsoft and third parties perform regular audits to attest that any access is appropriate. Access to encrypted customer data by Azure support personnel requires a customer's explicit permission and is granted on a "just in time" basis if needed. All accesses are logged and audited, and upon completion of the support task, access is revoked.

When a partner deletes a storage blob, what happens?

To understand how Azure handles data when it is deleted, let's first review how data is stored within Azure. For durability and high availability, data within Azure Storage accounts is replicated. Locally redundant storage (LRS) replicates data three times within a single facility within a single region for durability; geo-redundant storage (GRS) is replicated an additional three times in a secondary region. In Azure Storage, all disk writes are sequential.

This minimizes the number of disk "seeks," but requires updating the pointers to data objects every time they are written. A side effect of this design is that data cannot be deleted by overwriting with other data. The original data will remain on the disk, and the new data will be written sequentially. When a customer deletes a storage object (e.g., blob, file, queue, table), the pointer to this object is immediately deleted from the storage index used to locate and access the data. This operation is replicated asynchronously for GRS. With the storage index updated, the data is immediately unavailable. The sectors on the disk associated with the deleted data become immediately available for reuse and are overwritten when the associated storage block is reused for storing other data. The time to overwrite varies depending on disk utilization and activity, but is rarely more than two days. This is consistent with the operation of a log-structured file system. Azure Storage interfaces do not permit direct disk reads, mitigating the risk of another customer (or even the same customer) from accessing the deleted data before it is overwritten.

When a partner deletes a subscription, what happens?

If a subscription is cancelled or terminated, Microsoft will store customer data for a 90-day retention period to permit customers to extract data or renew their subscriptions. After this retention period, Microsoft will delete all customer data within 90 days of the retention period (i.e., by day 180 after cancelation or termination). If a storage account is deleted within a subscription, it is retained for two weeks to allow for recover1. y from accidental deletion, after which it is permanently deleted. NOTE: When a storage object (e.g., blob, file, queue, table) is itself deleted, the delete operation is immediate. To avoid retention of data after storage account or subscription deletion, customers can delete storage objects individually before deleting the storage account or subscription.

How does Microsoft dispose of hard disks?

Microsoft uses a disk disposal process that complies with NIST SP 800-88 R1, Guidelines for Media Sanitization. Disks are physically destroyed to render recovery of data impossible. Records of the destruction are retained and reviewed as part of our audit and compliance process. All Microsoft Azure services utilize approved media storage and disposal management services.

What should a customer do if unauthorized data is found to have been uploaded to their Azure storage account?

Azure implements safeguards for NIST SP 800-53 R4 control IR-9, Information Spillage Response; however, customers are responsible for data spillage incidents within their subscription and should refer to their internal incident response processes. Microsoft Azure Security Response in the Cloud outlines Microsoft and customer roles when responding to security incidents within Azure. Due to data striping across multiple disks, physical disks cannot be removed from service due to a customer data spillage incident. However, risk

associated with persistence of the data can be mitigated by deleting the associated storage blob, which makes the data unavailable and marked as available to be overwritten as discussed in question #4 above. Should a disk fail or reach end-of-life prior to an overwrite action, it will be destroyed as described above.

Could somebody physically steal my data?

Microsoft employs rigorous operational controls and processes to prevent unauthorized physical access to data centers, including 24×7 video monitoring, trained security personnel, key-locked server racks (housing compute, storage, and networking hardware), and smart card / biometric multifactor access controls. All physical access is logged. The way data is managed in Azure inherently includes several additional safeguards to help prevent access to data. For example, in Azure Storage, data is striped across multiple physical disks. Targeting specific data for theft would require not only knowing the correct data center, building, floor, room, and server rack on which the targeted data resides, but also understanding how the data is striped across disks and the location of each of the many physical disks where the associated strip units are written. In addition to these physical controls, Storage Service Encryption can be enabled to encrypt the data at rest, further preventing unauthorized access.

What additional resources has Microsoft published?

A variety of resources are available providing in-depth information about how customer data is stored in Azure. Check out the resources below for more information:

- Shared Responsibilities for Cloud Computing
- Protecting Data and Privacy in the Cloud
- Microsoft Azure Data Security (Data Cleansing and Leakage)

Enrollment

Who can access the Azure Secret Pricing Portal in the Partner IL6 environment? The initial partner account used to Create Tenant and Enrollment has Owner rights and full Billing Account access. Once the Partner is onboarded to MS-ISR they can give designated Data Plane accounts access to the billing account as well.

How are the data plane and mission place costs separated? Data and Mission Planes are in separate subscriptions, and they can be added to different billing or invoice sections on the high side for separation. It is up to the partner how to structure the billing account for cost management purposes.

Is billing information classified? The only cost data egressed to the low side is the rolled-up billing account total amount. This is a single number and is not split out by billing or invoice section, subscriptions, resource groups or resources. Detailed data is available for

reporting within the IL6 environment where cost management and billing tools are available.

Who controls who has access to the Il6 pricing portal and information in the pricing portal? Partner controls access to billing account and have the responsibility of managing all aspects including provisioning billing and invoice sections, licenses and subscriptions when required.

Identity

Does a partner need a new AAD tenant for every program and/or IRAD effort that wants to go into the Secret region?

A customer can achieve the required isolation leveraging rbac/policy/security groups for multiple mission owners to exist within one Azure Active Directory Tenant.

Can I have an IL6 only environment without having an IL4 environment?

Yes, MS-ISR can support an IL6 only deployment if that is the desired deployment pattern. However, the MS-ISR team recommends as a best practice to have an IL4 environment in addition, for testing, onboarding, training, development, etc. in the unclassified environment to then establish deployment pipelines from IL4 to IL6. This creates a DevSecOps pipeline low to high. But IL4 is not a fixed requirement for MS-ISR adoption in IL6.

Can the Partner build an identity structure in IL4 and then project that identity structure into IL6?

The Identity must be constructed and managed separately in each environment.

Is it possible to guest Azure Gov accounts from our existing tenant into the new Azure Gov MSISR tenant and then adding the guest objects to the baseline groups used for RBAC? Are there any downsides to this approach? Or do these accounts need to exist within the Azure Gov MSISR Active Directory and get synced up to Azure AD/Entra ID?

Data and Mission Plane Accounts must exist in AD and get synced up. We have a heavy reliance on AD and traditional based networking services throughout the ISR baseline due to a variety of factors we can go into further. Also, AVD doesn't work with Guest B2B accounts yet. Guest B2B account can be used for control plane management in IL4.

Release Management

Why is a partner unable to access the MS-ISR Project Site on Azure DevOps (https://aka.ms/msisr)?

This can be caused by multiple issues. First please ensure the request has been made to onboard the users to Azure DevOps.

Microsoft may be unable to onboard the partner if they are using accounts from their own Azure Active Directory and have Cross-Tenant collaboration access with microsoft.com disallowed. The partner will need to allow users to be guested, via cross-tenant B2B, into the microsoft.com tenant for access to the MS-ISR Azure DevOps site.

If the partner has both Commercial and GCC High Tenants available they should use the Commercial account to request access.

Security

If we need to use a HSM for our PKI how would that be enabled in MSISR or is there a HSM service we could consume?

Support for HSM is available, please submit a request to MS-ISR team to enable within codebase.

Are there any compliance issues regarding the use of Azure Update Management Center in MS-ISR? Are we clear to orchestrate our patching strategies with it without any issues?

Partner is responsbile for all Patching and System updates. Update Management/Update Management Center isn't authorized for use Azure Secret IL6. Partners will have to implement their own patch management processes/tools including implementing a Partner Managed CDS to move updates from low to high environments.

Platform Administration

What are the SLAs available for Azure Secret?

Azure Secret is subject to the same standard/worldwide Azure SLAs

What Linux Distributions and Repos are available in MS-ISR?

The following repos (universe/multiverse/extras) are mirrored with Yum services deployed as part of the default MS-ISR environment:

- CentOS 7
- RHEL 7
- RHEL 8 Afterward these repos are automatically synchronized on a weekly basis.

For all other Distros the partner must bring their own update solution via partner owned CDS solution.

Where can I find documentation on the Control Plane/Data Plane?

See Platform Administration section in Wiki.

What specific parts of an MS-ISR IL4 environment are replicated in IL6? What things can be directly duplicated and what things are specific to IL6?

Everything in IL4 can be replicated in IL6. In other words, we don't do anything in IL4 that we can't do in IL6.

What specific things would Microsoft recommend Partner teams be doing in IL4 to prepare for standing up their MS-ISR instance in IL6?

See the Data Plane Admin Guide, it has the data plane team requirements, configurations and level of effort. It is also recommended to identify a Mission Owner to pilot the deployment of an application in the Mission Plane and have them refer to the Mission Plane Admin guide to get started.

Are the services listed in the Data Plane you had in the diagram only there to support the AVD to jump into the Mission Plane or are they shared between the two?

The Data Plane provides intermediary connectivity and management services utilized by Mission Plane instances based on requirements outlined in the DoD SRG and Secure Cloud Computing Architecture (SCCA). including Management and Collaboration Services (VDSS and VDMS Components). Additional 3rd Party services are included based on customer requirements.

From the AVD in the Data Plane are we free to use any automation tooling against Azure?

This environment has no internet access and has a very limited Azure store. In theory if you need to use a specific tool and it can be run without connectivity to external dependencies then you can use it once you have brought it into the environment. Due to the way the environment is set up the configuration of any tooling may need customisation.

There are specific instructions provided for installing and running a variety of tools including vs code, python, powershell, bicep, terraform, ansible and more.

Do we need to install agents or send log streams out of our Enclave, to a SNOC to comply with US security requirements?

Approved and authorized connections for general transport. DCSA / Authorizing Authority / Partner need to go through an approval process for any additional connections.

Already approved thin client connection to AVD and supporting services to that (DNS, ADFS etc…)

Private peering combined with public peering. Public is authorised endpoints. Private peering is the supporting services for AVD.

Are there any restrictions on DNS naming of our solution components in the Enclave? E.g., could we use a TLD like .internal or .local?

Yes, easiest path is to use a Microsoft.scloud namespace in the data plane. Mission plane can be anything and can be multiple forests.

Are there restrictions on COTs binaries that we ingest into the AVD to build our solution? I.e., do we have to supply them via an impex process or once connected can we consume the AVD in the Data Plane like normal Azure and upload whatever we want into the Enclave?

Anything not already available in US SEC to consume via the Azure Store or shared container registries/image galleries needs to be brought in through a suitable inpex process.

There is no 'store' capability as yet but several images are made available as part of the ISR deployment.

Does the AVD come installed with the Azure cli or Azure Storage Explorer?

Yes

Do we own and manage the AVD in the Data Plane? Can we install automation tooling on it and bring it under management of a Domain we create in our solution?

AVD is installed as part of the provisioning then passed to the 'customer' to own and run.

Under a sponsored tenant this sits with the responsibility of the sponsor.

Can we deploy additional AVDs in the Data Plane for management of our solution in the Mission Plane or do these need to be in the Mission Plane?

Yes. Data Plane admins can add additional hosts to the Data Plane AVD Host Pools using the supplied Template Specs. New Host Pools or App Group requests should be submitted to the MS-ISR Platform Team for deployment.

A dataflow we require is to have a jump server that executes the automation against Azure but also reads metadata or secrets from the services we deploy within our solution. Can this dataflow be supported from the AVD in the Data Plane or is Azure front-end access and "tenant" service access split at the network level?

Rather than use AVD it might be better to run virtual machines as a shared service to support this need. These can have vNets peered to allow access to all the required metadata.

Is Blob storage created in the Mission Plane or the Data Plane?

Blob storage can be created in both.

What Configuration Management Utilities will work against MS-ISR?

Typically any provider that work with Azure Government or Commercial will work with Azure Secret (ex. Terraform, Ansible, Python, Azure CLI, PowerShell, ARM/Bicep, etc...) In many cases the default API endpoints used with the SDKs needs to be adjusted to use the Azure Secret Endpoints. See Mission Plane Admin Guide for detailed guidance.

What Resource Types, VM Sizes and Extensions are Available in MS-ISR?