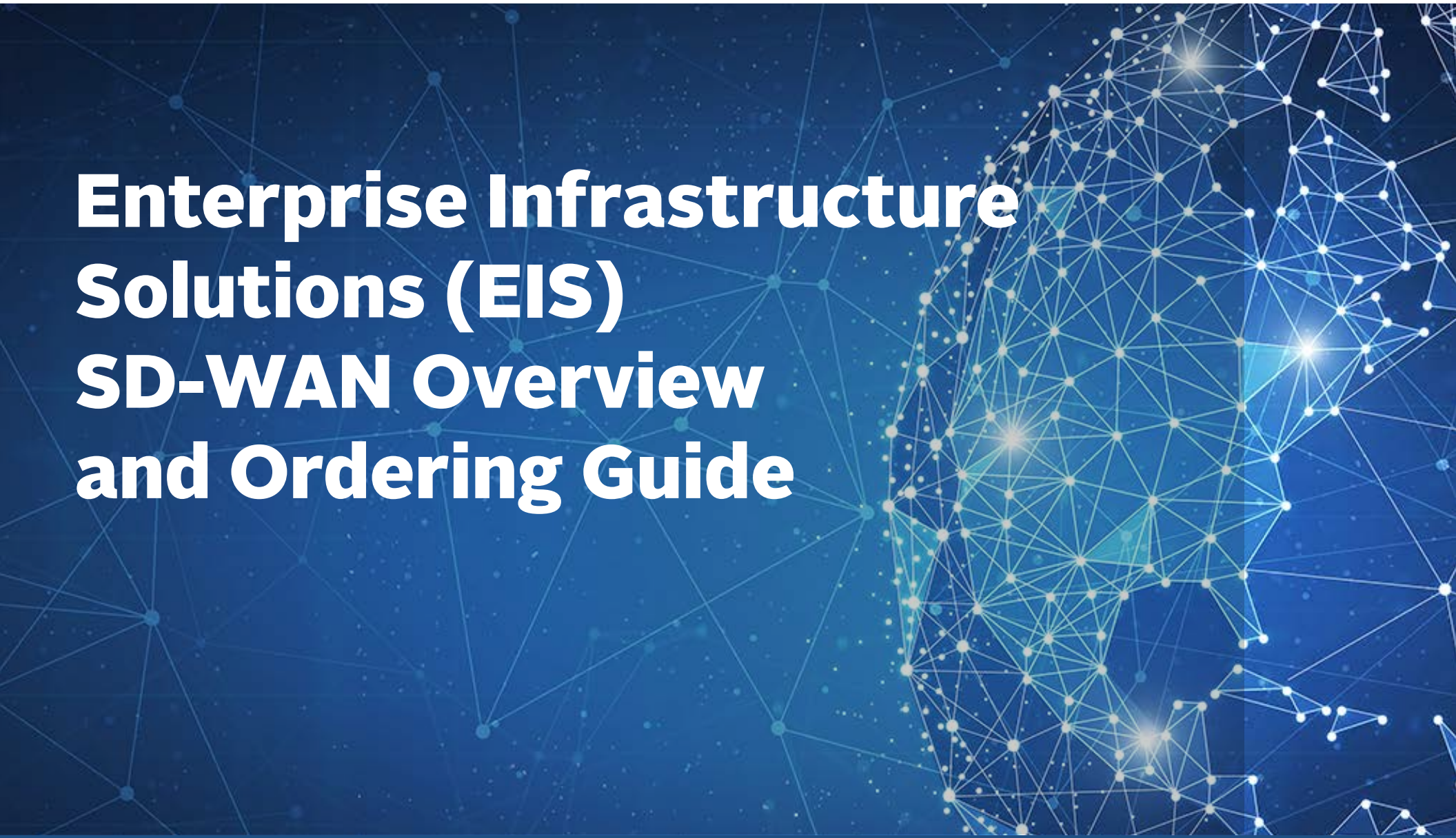
U.S. General Services Administration
Federal Acquisition Service (FAS)
Information Technology Category (ITC)
Enterprise Technology Solutions (ETS)
Technical Account Management Division (TAM)
Solutions Development (SD)



Enterprise Infrastructure Solutions (EIS) SD-WAN Overview and Ordering Guide

VERSION 2.0

AS OF JUNE 2024

Table of Contents

1. Introduction

This SD-WAN Overview and Ordering Guide (guide) is to assist Federal agencies in implementing Software-Defined Wide Area Network (SD-WAN) technologies under the Enterprise Infrastructure Solutions (EIS) contract. The primary target audience for this guide is Federal decision-makers considering whether and how to incorporate SD-WAN into their telecommunications networks. This guide incorporates information from industry providers and the Metro Ethernet Forum (MEF) Forum, the industry's first voluntary SD-WAN standard – SD-WAN Service Attributes and Services (MEF 70) – initially published in July 2019 (hereafter "MEF 70"), and since updated versions 70.1 and 70.2; and related security (MEF 88), and unified policy framework standards (MEF 95).

SD-WAN is an application-driven architecture designed to simplify the management of a Wide Area Network (WAN). The SD-WAN overlay is not dependent on dedicated hardware connections and can easily distribute network traffic across the enterprise. SD-WAN is a cost-effective, reliable, and secure solution that improves performance through automation and greater visibility. Certain market drivers are pushing enterprises to adopt SD-WAN, including the following:

1. High-cost legacy networks (most frequently, Multiprotocol Label Switching (MPLS)-based) that aren't keeping pace with dramatically rising bandwidth demands, particularly from video and cloud-based Software-as-a-Service (SaaS) and Network-as-a-Service (NaaS) applications.
2. Inflexibility and/or poor quality of service (QoS) from legacy networks and the need for more centralized network monitoring and management capabilities.
3. Backhaul of traffic from branch/remote locations to headquarters or centralized data centers result in expense and inefficiencies to meet cybersecurity requirements.
4. Overcoming cybersecurity vulnerabilities/challenges that have made the traditional "perimeter" network defense strategy inadequate.
5. Transforming the networking environment with the latest holistic solutions such as Secure Access Service Edge (SASE), which integrates five core components: SD-WAN, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), and Zero Trust Network Access (ZTNA).

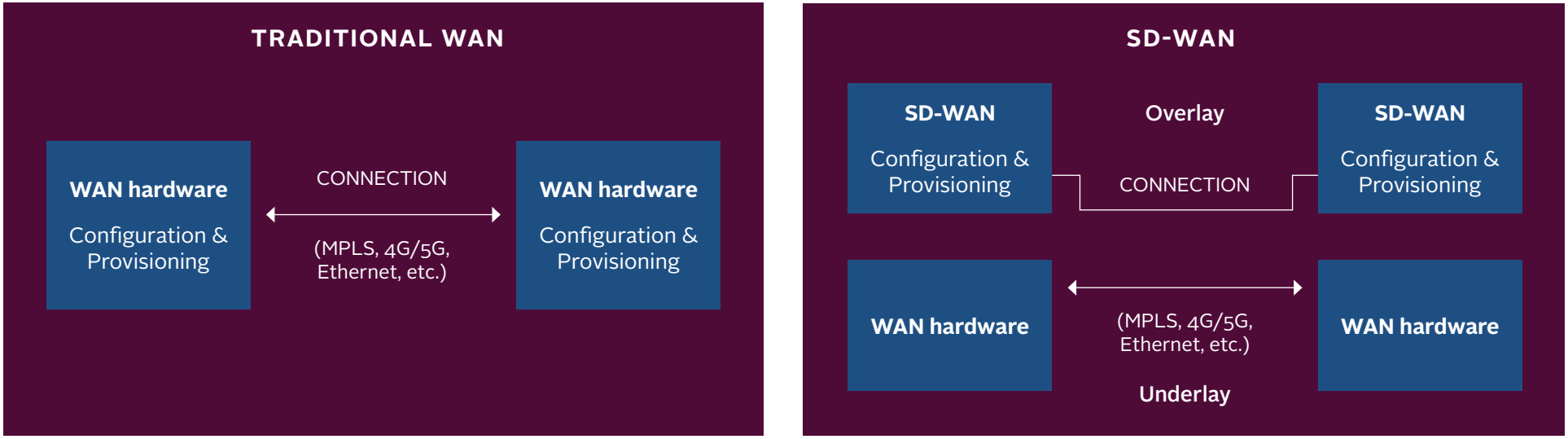
SD-WAN is a key industry technology, along with cloud-based applications and infrastructure, for enterprises to modernize their networks and keep pace with the telecommunications demands of their workforce and external clients. The SD-WAN overlay, or managed service component, is key to this evolving and innovative security and cloud-based solution.

The SD-WAN architecture is ideal for a Federal agency relying more heavily on cloud-based applications. It avoids the expense and quality concerns associated with backhauling data through a centralized data center. SD-WAN allows for more integrated, in-depth cybersecurity that can meet evolving Federal security requirements if properly implemented and continually monitored. An evaluation of the agency's IT resources and the complexity of its networking needs is essential to determine the best option to meet agency needs.

1.1 OVERVIEW OF SD-WAN TECHNOLOGY

SD-WAN is a virtual WAN network architecture that utilizes various data transport technologies and a centralized control function to connect users securely and intelligently to applications. Unlike traditional WAN, SD-WAN de-couples the transport service from its applications and software control function, resulting in a more agile, reliable, and cost-effective network architecture. SD-WAN acts as an overlay network to monitor, manage, and optimize the use of that transport. The SD-WAN overlay provides software control that operates as a separate plane from the underlying network transport functions.

FIGURE 1 THE SD-WAN OVERLAY (TECHTARGET)



A traditional WAN requires hardware at each network end to complete the connection. An SD-WAN overlay sits on top of this connection but it does not replace it. SD-WAN abstracts control of the WAN connection into a software layer, as configuration and provisioning split into a separate plane[1].

1.2 DEFINING CHARACTERISTICS OF SD-WAN

MEF 70 defines SD-WAN in terms of seven fundamental characteristics:[7]

1. A Secure, IP-based Virtual Overlay Network: SD-WAN does not replace, or even modify, the data transport network(s) upon which it relies, such as an existing MPLS-based WAN. Instead, it creates and manages an overlay network that utilizes virtual connections riding the existing transport. Typically, SD-WAN uses IPSec tunnels8 through MPLS or Internet underlay networks.

2. Transport-Independence of the Underlay Network(s): SD-WANs can operate over any type of digital transport network, including MPLS; carrier Ethernet; the public Internet, as accessed by best-effort broadband services or Dedicated Internet Access ("DIA");9 wireless such as 4G LTE and 5G (as the latter becomes deployed more widely); and satellite-based transport.

3. Quality-of-Service (QoS) Assurance: Monitors in real-time key QoS parameters (latency, packet loss, etc.) set by the network manager, ensuring the specified performance level is maintained.

4. Application-Driven Packet Forwarding: SD-WANs can distinguish data flows by the application they support. This capability allows users to select which underlay transport option a given application utilizes. (This is a specific instance of the "Policy-based Packet Forwarding" characteristic discussed below.)

1 – TechTarget* TIP, Before deploying SD-WAN, assess your underlay network components, 13 Mar 2020.

5. High Availability through Multiple WANs: SD-WANs support packet forwarding over multiple WANs at each site.10 Each WAN underlay network can use a different wireline or wireless access provider, providing transport diversity and increasing overall connectivity availability.

6. Policy-based Packet Forwarding: SD-WANs can apply customized networking policies to packet flows. This customization means users can choose their desired quality-of-service, security, and/or business policy, and their traffic flows over the best-matching transport underlay and overlay.

7. Service Automation via Centralized Management, Control, and Orchestration: SD-WAN offers centralized management capabilities, typically accessed via a web portal or Application Programming Interface (API). The various network roles (e.g., service provider, network administrator, network user) perform real-time network monitoring and administration at varying levels of access and control. A novel aspect of this centralized management is that SD-WAN enables "zero-touch provisioning" of Customer Premises Equipment (CPE): When a new SD-WAN CPE powers up and connects, it can retrieve its configuration and policies without needing to send a service provider installer to the site.

1.3 SD-WAN REFERENCE ARCHITECTURE

The SD-WAN architecture is composed of key components (planes responsible for specific networking processes.

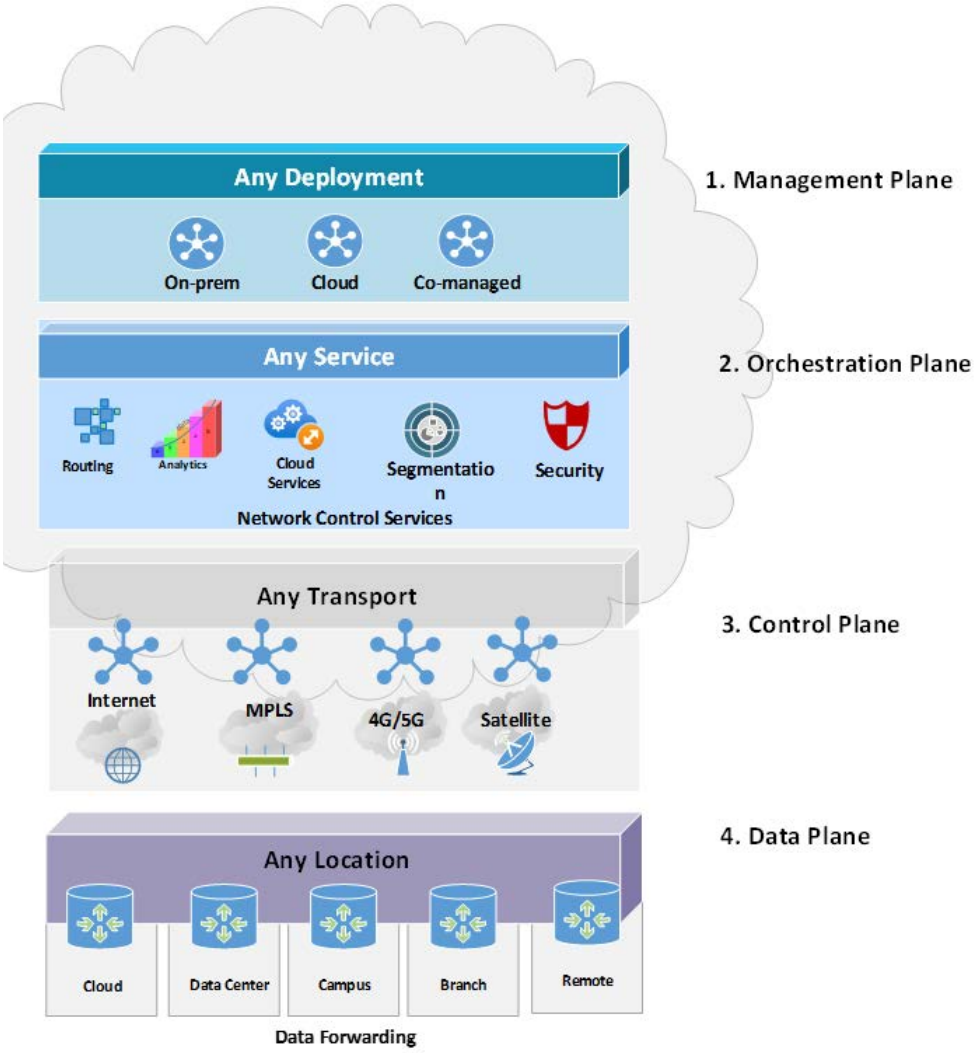
The **Management plane** runs the system's user interface and operates as a dashboard for network administration. It administers an agency SD-WAN deployment, whether On-premise, Co-managed, or cloud-based. The edge devices alert of any events or outages and overlay the traffic engineering policies.

The **Orchestration plane** combines all components to build a Datagram Transport Layer Security (DTLS) connection to network applications and services.

The **Control plane** controls how data packets move between locations and creates, monitors, and manages routing network paths. An agency can combine and integrate multiple data transport technologies (MPLS, 4G/5G, Internet, satellite, etc.) controlled using SD-WAN software and edge devices for dynamic traffic routing, prioritization, and policy-setting capabilities.

The **Data plane** (or forwarding plane) routes and forwards the data packets across the WAN to the edge of the endpoint location. The Control plane sets the policies for the Data plane.

FIGURE 2 SD-WAN DEPLOYMENT



2. Why SD-WAN?

This section reviews the marketplace factors driving enterprises to adopt SD-WAN, the technology's benefits and potential risks, and some examples of how a Federal agency could use SD-WAN to improve its delivery of network capabilities. SD-WAN allows agencies to adopt an integrated approach to network and data security, including such elements as native next-generation firewall (NGFW) functionality, encrypted virtual private network, high-performance Secure Socket Layer (SSL) inspection, and Transport Layer Security (TLS).

2.4 MARKET DRIVERS FOR SD-WAN ADOPTION

Many private sector enterprises and some forward-thinking public sector agencies15 have been turning to SD-WAN as a highly effective solution to several widespread networking problems.

- Based on a review of public case studies undertaken on behalf of GSA,16 the most frequently cited driver leading enterprises to deploy SD-WAN is their reliance on a legacy network (most frequently, MPLS) that is high-cost and incapable of providing the bandwidth speeds demanded by today's bandwidth-intensive applications.
- A second common driver of SD-WAN adoption is quality of service problems (e.g., network outages) with the customer's legacy telecommunications networks and the need for more visibility and control over the network. Numerous case studies attribute lost sales/profits and other business-impacting effects to poor service quality.
- A third common problem driving SD-WAN adoption is a decentralized, disaggregated information technology (IT)/telecommunication infrastructure with no centralized management or monitoring capabilities.
- A fourth common driver of delayed, slow market roll-out or limited location placement of SD-WAN adoption is a dependence on carrier provisioning of lines or circuits.
- A fifth common reason for SD-WAN adoption is the need for the legacy system to backhaul traffic from branch/remote locations to headquarters or centralized data centers, leading to inefficient traffic routing and potential failure points.

As identified by enterprises, other SD-WAN drivers include overcoming cybersecurity vulnerabilities/challenges and increasing demand for cloud-based applications. Moreover, routing cloud-based services traffic through a common data center, as typically occurs in a traditional WAN, degrades performance and unnecessarily consumes bandwidth. SD-WAN allows direct routing to/from cloud-based services, increasing networking efficiency without compromising cybersecurity.

2.5 SD-WAN BENEFITS AND RISKS

SD-WAN is a major innovation that can improve WANs' performance and solve the most common problems when using a traditional WAN. At the top of the list of its benefits, SD-WAN can enable an agency to connect multiple sites via a secure, flexible set of WANs and choose the most cost-effective transport options available to meet each site's particular requirements. For example, agencies can replace expensive, high-performance MPLS circuits with cheaper, best-effort broadband Internet or wireless 4G LTE connectivity for some sites and applications.17 The cost savings are substantial, given that MPLS price levels (e.g., measured per 100 MB of bandwidth) can be an order of magnitude higher than those Internet and wireless alternatives.18 Additionally, SD-WAN can provide significantly better network performance than traditional WANs when measured along the dimensions of agility, scale-ability, service availability, and resiliency.

For example:

- SD-WAN allows agencies to adopt and enforce network-wide policies with respect to security, least-cost routing, and SLAs. Attempting to do so in a traditional WAN context is often impractical and expensive since it would require site-by-site, hands-on interventions instead of the near-instantaneous, one-time adjustments afforded by the SD-WAN controller and Subscriber Web Portal/API.
- SD-WAN gives end-to-end, real-time network monitoring capabilities through dashboard-type access, i.e., visibility through a single pane of glass. Depending upon the chosen degree of agency control (i.e., DIY vs. Managed Service options), that visibility can translate into extensive real-time adjustment of network-wide policies, providing an unprecedented level of agility when compared to a traditional WAN.
- Similarly, SD-WAN's "zero-touch" capability allows agencies to undertake fast and simplified set-up/take-down of network "edge" locations. This capability is a compelling advantage for agencies that experience rapid turnover of remote locations needing access to their network. With "zero-touch" and the routing flexibility enabled by its network-wide policy application, SD-WAN can scale the network's reach and capacity much more rapidly and completely than a traditional WAN.
- SD-WAN can greatly improve network resiliency and overall network uptime by using multiple data transport technologies that use physically distinct facilities for diversity in a blended, seamless fashion via its dynamic policy control capabilities.

2.6 EXAMPLES OF HOW SD-WAN CAN BE USED

Private sector enterprises' experiences illustrate several ways a Federal agency could improve its networking capabilities and efficiencies through SD-WAN. Some of the best examples are summarized below:

- Agencies can overcome reliance on a legacy network (often MPLS) that is high-cost and incapable of providing the bandwidth speeds demanded by today's bandwidth-intensive applications. While MPLS networks can provide the highest QoS and reliability, they are among the highest-cost transport options, partly because they typically require a hub-and-spoke architecture in which all traffic is backhauled to the hub data center(s). SD-WAN can separate traffic flows by application and/or network policy, allowing less-critical traffic to traverse cheaper data transport technologies, such as broadband Internet or 4G-LTE/5G wireless, without backhauling.
- Agencies can quickly scale up/down network scope and bandwidth to meet rapidly- changing demand. A key strength of the SD-WAN is its scale-ability. Users can configure their networks to add/drop circuits and bandwidth in real-time through direct control of the SD-WAN central dashboard (in a co-managed arrangement) or via their vendor (in a Managed arrangement). Similarly, connecting new agency branches and field locations in hours to minutes with two broadband Internet connections and an "Edge" device without trained technicians, instead of taking weeks or months as with a traditional WAN.
- Agencies can provide secure connectivity to geographically distributed locations: Agencies can use SD-WAN to make secure, high-speed, and flexible connections between headquarters, data centers, field offices, and other diverse locations, enabling agency personnel and remote users to access agency resources securely.
    - An agency could use SD-WAN to enable remote offices to connect to the agency's intranet securely.
    - An agency with many teleworkers or field agents could use SD-WAN to enable remote and mobile personnel to securely connect to their cloud-based accounts and applications over an encrypted connection. This secure connectivity gives workers access to the same information and IT assets that they would have sitting at their desktops. Compared to traditional WANs, SD-WAN enables greater flexibility and cost-efficiency.
    - Use SD-WAN to enable authorized private and government partners to gain access, via a secured agency extranet, to agency applications and data.
- Agencies can integrate SD-WAN with other network and security options in the cloud to transform their enterprises. SD-WAN is one of the five core components of a SASE operating environment, integrating cloud-based firewalls and software with a zero-trust network approach.

3. Is SD-WAN Right for You? A Checklist for Initial Evaluation

There are many factors to consider when evaluating whether your agency should adopt an SD-WAN solution. The following checklist serves as an initial, high-level guide during decision-making by highlighting some of the considerations that typically bear the most weight, as seen in public case studies and use cases for SD-WAN. Of course, each agency should consider its circumstances, including its present and future telecommunications needs, budgetary and personnel resources, and the status of its network infrastructure.

Checklist for Agency Consideration of SD-WAN Adoption

1. Does your agency have (or can obtain) sufficient budgetary resources to start implementing an SD-WAN overlay?
2. Is using the public Internet and/or wireless transport options consistent with your agency's System Security Plan?
3. Is your agency free from other operational considerations (e.g., low latency requirements) that would deter or prevent it from using the Internet or wireless transport? (Consider QoS improvements SD-WAN's dynamic control can bring, e.g., tunnel bonding, Forward Error Correction, etc.)
4. Is your agency's traffic profile a mix that could benefit from disaggregating into higher-valued vs. lower-valued communications by applying different policies for priority, QoS, and/or security?
5. Is your agency using, or planning to use, a significant volume of cloud-based applications?
6. Are you experiencing capacity constraints on your existing WAN that make it difficult to overcome within its current architecture?
7. Do you forecast (or have qualitative reasons to anticipate) a substantial increase in traffic volumes for your existing WAN over the next few years?
8. Has your existing WAN had significant reliability issues that a SD-WAN solution could mitigate by integrating additional transport options for route diversity, redundancy, and backup?
9. Does your agency experience significant turnover (additions/eliminations) of branch offices or other user locations that require network personnel to go on-site to effect those changes?

The first two items on the checklist are key considerations for determining whether your agency is ready for SD-WAN. If meeting baseline conditions, then saying "Yes" to any combination of the seven factors that follow, or even one or two, may suggest that you should seriously consider adopting SD-WAN for your network.

In that case, the next step is to undertake an in-depth network assessment, covering both the existing network infrastructure and current demand profiles, plus forecasted changes in demand (considering cloud migration, data volume growth, etc.) to better understand your agency's needs. An in-depth network assessment is completed internally or with the assistance of third-party consultants with the necessary expertise. Review the results of the network assessment against the checklist information and any additional considerations of importance to your agency to reach a decision about whether to proceed.

4. SD-WAN Implementation Deployment Use Cases

Implementing SD-WAN is a tricky decision for Federal agencies. There are multiple options, and not all providers are alike. While some have built their solutions internally and have an excellent working knowledge of how it works, others are simply reselling SD-WAN products. The EIS Contract Software Defined Wide Area Network Service ("SDWANS") accommodates the vendors' provision of fully Managed and Co-Managed SD-WAN solutions. Integrating other EIS services, such as the Software-as-a-Service (SaaS), can enhance these offerings. An agency must consider its overarching information technology objectives when determining the best deployment strategy. This section explores four deployment strategies: On-premise, Co-managed or hybrid, cloud-based, and Secure Access Service Edge (SASE).

4.1 USE CASE 1: ON-PREMISE SD-WAN

The On-premise deployment is for agencies that want to manage the network and leverage hardware (HW) appliances at the edge, in data centers, cloud services, and at agency locations. HW appliances manage network traffic, with policies and configurations managed via a web application within the existing network connections (e.g., MPLS, Broadband, fiber, satellite, or wireless). The edge devices reside at the enterprise locations, and management is completed by the agency or remotely by a service provider.

RESOURCE EXPERTISE: Requires agency resources to have comprehensive expertise to handle all organization operations.

DEPLOYMENT COST: The agency must invest substantially in acquiring, setting up, and maintaining the necessary infrastructure, resources, and tools. An on-premise approach allows the agency to leverage existing IT assets to maximize the return on investment.

NETWORK MANAGEMENT RESPONSIBILITY: The agency is fully responsible for the network's design, implementation, and management. The on-premise approach requires a dedicated team to monitor, maintain, and optimize network functions. The agency is responsible for SD-WAN equipment, edge devices, network connections, and software. The agency has direct control over network configurations and HW appliances with the flexibility to tailor the SD-WAN solution.

CHALLENGE: A common issue is whether the agency IT network and engineering personnel are available and have the appropriate skills and experience to deploy and maintain an SD-WAN environment.

4.2 USE CASE 2: SD-WAN HYBRID (CO-MANAGED)

One of the most prevalent SD-WAN use cases for private enterprises involves a hybrid or co-managed network operating on the agency's transport underlays. While the traditional MPLS network usually provides highly reliable and secure connectivity, its connections are relatively costly, and adding or deleting sites to an MPLS network is time-consuming. SD-WAN can establish encrypted paths through the underlay network to provide connectivity. Many federal agencies already have an MPLS network, making it relatively easy to transition to this type of hybrid configuration. The SD-WAN co-managed option lies between an on-premise approach and a fully managed SD-WAN.

A co-managed solution can take systems management off the task list for enterprise IT while still allowing them the required control to make changes as needed. Agencies that view security as a priority can continue to control the administration and monitoring of SD-WAN policies to ensure they are well-suited for the enterprise. Federal agencies may find that a Co-Managed SD-WAN provides the optimum balance by leaving the management of the basic infrastructure to the service provider but retaining hands-on control of key functions such as setting network policies, allocating bandwidth, and turning up new branch offices and other remote sites.

RESOURCE EXPERTISE: The agency partners with the provider and can access external specialists to fill any knowledge gaps or areas that require additional assistance. This method allows the agency to leverage internal and provider expertise as needed and retain direct control of specific aspects of the network. In-house skills and capabilities are evaluated before selecting this option.

DEPLOYMENT COST: Start-up costs vary based on the scope of the partnership with the provider.

NETWORK MANAGEMENT RESPONSIBILITY: The provider focuses on the day-to-day management of the network, while the agency can focus on control over decision-making, policies, and specific segments of the network. The agency maintains control of critical functions and may maintain control of some SD-WAN overlay functions. Balancing the responsibilities between the agency and provider is based on scope requirements.

CHALLENGE: The collaboration process between the agency and provider is challenging and requires clearly defined roles and responsibilities for managing the network.

4.3 USE CASE 3: SD-WAN CLOUD-BASED

The SD-WAN Cloud-based solution uses a cloud-based virtual appliance in conjunction with edge hardware appliances. This deployment method is cost-efficient and alleviates the need for the agency to obtain internal specialists or invest in hardware. A cloud-based solution uses a central cloud instance that routes and manages remote (edge) location traffic through WAN connections. The provider works with the agency to define the network design and security configurations.

The cloud-based solution utilizes management software to implement the SD-WAN features, which are communicated to the edge appliance via a web application (orchestrator) to keep the cloud solution and edge components in sync. A cloud-based architecture offers better performance for agencies accessing cloud-based applications because SD-WAN locations connect to a virtual cloud gateway over the Internet. The cloud-based option is easily scalable and is flexible to keep up with an agency's expansion and adjustments to the network infrastructure.

RESOURCE EXPERTISE: The agency has access to external experts, relieving the requirement for in-house knowledge.

DEPLOYMENT COST: Reduces the upfront expense of SD-WAN infrastructure deployment and procurement of edge devices.

NETWORK MANAGEMENT RESPONSIBILITY: The provider manages and monitors the network agency requirements, including specific criteria to ensure critical functions and enforce security policies. Vendor-agnostic and carrier-agnostic providers can more effectively adapt and mitigate constraints and vulnerabilities by using a cloud-based virtual appliance in conjunction with edge hardware appliances.

CHALLENGE: The agency may have limited direct control over the SD-WAN infrastructure and must rely on the service provider for network quality, performance, and security.

4.4 USE CASE 4: SD-WAN SECURE ACCESS SERVICE EDGE (SASE)

SD-WAN is one of the five core components of a Secure Access Service Edge (SASE) solution. The SASE concept is the latest in enhanced security strategies and advanced tool sets that provide protection to all users, devices, data, infrastructure, networks, and assets, no matter who is accessing them. SASE integrates

network and security components into a single cloud-based service, improving accessibility, security, and controls. The increase in visibility and "real-time" control available to agencies offers the ability to optimize traffic using SASE tools' enhanced capabilities.

Agencies using a SASE approach to implement SD-WAN, with a Zero Trust Access approach, enhance network management capabilities, offer faster application of changes, and ensure security regardless of where or how a user connects. The core SASE components are essential to managing and protecting network traffic, users, applications, devices, and infrastructure. The SASE technical specifications are unique to each agency's enterprise architecture and are an integration of the five core SASE components:

- **Zero Trust Network Access (ZTNA)** protects remote users and enforces security policies dynamically, utilizing an identity and access management process at network-segmented policy enforcement points where devices, endpoints, applications, and applying data security.
- **Cloud Access Security Broker (CASB)** protects cloud-based data using on-premises or cloud-hosted software or hardware between the cloud solution provider and the end-user.
- **SD-WAN solutions** provide centralized management and visibility. They use software-defined networking concepts to distribute network traffic across the network and connect branch offices and users to agency data centers or cloud-based and SaaS applications.
- **Secure Web Gateway** (SWG) – Designed to implement and enforce an organization's web security policies and defend against malicious web traffic and malware. An SWG utilizes an on-premise or cloud-based service between the user and the Internet to inspect web requests and block malicious applications and websites, making them inaccessible.
- **Firewall as a Service** (FWaaS) – Secures WAN and LAN traffic using a cloud-based service that provides hyperscale, next-generation firewall (NGFW) capabilities, including web filtering, advanced threat protection (ATP), intrusion prevention system (IPS), and Domain Name System Security (DNSSEC)[2].

Expanding the SD-WAN implementation method using a SASE approach allows agencies to optimize and modernize their operating environments fully. SASE allows agencies to release themselves from the limitations of service delivery dependent on legacy hardware-based networks and data center-driven architecture. These advantages are true even with a network-delivered set of cloud services. Implementing SASE expands user connectivity options and offers flexibility when accessing information systems. SASE modernizes the entire enterprise network environment.

RESOURCE EXPERTISE: SASE deployment uses a single vendor, multi-vendor, or hybrid approach that allows the agency to leverage the expertise and knowledge of more than one provider and on-premise resources.

DEPLOYMENT COST: While a single provider SASE solution has a lower total cost of ownership, the benefits of utilizing a solution that leverages multiple vendors may find efficiencies in other areas by offering best-of-breed options.

NETWORK MANAGEMENT RESPONSIBILITY: A single provider deployment offers simplicity and ease of management but may leave the agency locked in with one vendor with limited choices and flexibility. The multi-vendor approach provides best-of-breed options but is more complex and may have varying levels of interoperability, disjointed administration, and higher traffic latency. The hybrid approach offers access to specialized expertise and greater flexibility. Still, it may result in separate network and security teams, integrated interoperability, and increased network latency that may impact the user experience.

CHALLENGE: SASE is a complex solution that requires matrixed collaboration among network and security teams and key stakeholders on requirements.

2 What is FWaaS?, Fortinet

4.5 DEPLOYMENT COMPARISON SUMMARY

Evaluating the agency's IT resources and the complexity of its networking needs is critical to determining the best approach. The agency's size and number of locations are often driving factors in selecting a provider with adequate coverage and the ability to provide local support when needed. The table below summarizes the pros and cons of the four SD-WAN use case deployment methods.

An agency selecting an SD-WAN deployment method is an important decision and needs careful consideration. SD-WAN is perfect for agencies that may need to migrate incrementally. Engage all stakeholders in key budget, transport, and security areas as part of your enterprise operational assessment to develop SD-WAN requirements. Determining whether the agency has the necessary resources and experience should drive the decision to keep partial or full control of the agency or whether outsourcing SD-WAN in full or partially is the most beneficial success. Moreover, the agency's future IT goals may determine if a cloud-based solution or SASE is best to deliver a comprehensive and efficient SD-WAN deployment.

TABLE 1 SD-WAN DEPLOYMENT METHOD PROS AND CONS

Deployment Method	Pros	Cons
On-Premise	• The agency controls network traffic flows with subscription services • Easier to scale appliances to meet varying needs across the enterprise • Offers low latency routing for any traffic, especially between locations • Edge devices have all the intelligence needed for traffic prioritization and routing decisions	• The agency responsible for the acquisition of required bandwidth • Deployment is reliant on detailed knowledge of network architectures • Optimization across platforms is challenging, and interconnects to major cloud/SaaS providers may not be available • Can not present a single IP when connecting to cloud services
Hybrid or Co-managed	• Reduces burden to agency IT operations for network management • Easier to integrate with broader SD-WAN toolsets • Changes are software-driven; easier porting from one place to another • Flexible license management scalable to changing needs	• Requires extensive expertise to deploy and manage • Most effective on an established, mature virtualized network • WAN management may not fully optimize hardware
Cloud-based Service	• Easy to deploy with simple edge appliance controlled in the cloud • Integrate Network-as-a-Service (NaaS) into the solution for enhanced efficiencies • Better control over cloud application performance with data center • Static IP addresses obtained from the SD-WAN provider • SD-WAN software can reside anywhere a virtual environment is present (Headquarters (HQ), data center, remote locations)	• All network traffic goes through the cloud before the enterprise and can add latency when remote sites try to reach agency HQ or data center systems • Limited bandwidth scalability at the edge due to simple hardware • Limited routing and configuration options and not suitable for complex networks • It may not support both public and private WAN connections
SASE	• Offers a comprehensive and innovative cloud-based network and security solution based on integration • Enhanced security capabilities to address emerging cybersecurity threats and vulnerability of WAN endpoint devices • SASE integrates five core components: SD-WAN, Zero Trust Access, Firewall-as-a-Service, Secure Web Gateway, and Cloud Access Security Broker • Enables network performance and optimization • Offers increased agility, greater network visibility, and controls while enhancing the overall user experience • Consolidation of network and security in the cloud is a cost-effective strategy	• Integrating legacy with cloud-based platforms is challenging • This can create a fragmented and confusing ecosystem • Performance of network security protocols and fragments in a cloud environment • Complexities of procurement

5. Ordering and Pricing Basics for SD-WAN

The EIS services portfolio includes Software-Defined Wide Area Network Service (SDWANS), which is a Managed Services (MNS) offering (*See* EIS Contract Sections B.2.8.10 and C.2.8.10 (SDWANS). The MEF 70.2 standards aligned with using EIS service offerings to determine the specific services ordered. The key ordering components for SDWANS include the transport services for the Underlay network, MNS underlay/overlay software, configuration options for network visibility and monitoring, and Service Related Equipment (SRE). The equipment used for SD-WAN will need to have greater processing power than traditional network hardware and additional memory capacity to run both the underlay and virtualized overlay network.

Note: Please see the EIS Acronyms and Abbreviations and the EIS Glossary for clarification of terms and acronyms used in this document. See also MEF 70, Section 3, Terminology and Abbreviations.

5.1 KEY ARCHITECTURAL SPECIFICATIONS

The EIS SD-WAN service offering includes key architectural specifications listed below, with specific capabilities and optional features described in the EIS Contract (Section C.2.8.10 SDWANS). Please visit the EIS Service Guides to better understand the EIS SD-WAN service offerings and pricing fundamentals. The SD-WAN service guides describe the key architectural and technical capabilities and features. The pricing structure for SD-WAN depends on obtaining it as an on-premise, Hybrid (co-managed), or cloud-based solution.

Underlay Transport Network—The underlay transport network is any IP network, including contractor-provided Enterprise Infrastructure Solutions (EIS) services such as the Virtual Private Network Service (VPNS), Ethernet Transport Service (ETS), Internet Protocol Service (IPS), Broadband Internet Service (BIS), and Managed Wireless Service (MWS). The SD-WAN Gateway function permits intercommunication between VPNs beyond the boundaries of the SD-WAN itself.

EIS CAPABILITIES AND FEATURES

- **Routing Requirements** (Section C.1.8.8) – Ensuring applied and proxied encrypted tunnels to allow inspection.
- **Commercial BIS** – Provides optional BIS when specified in the Task Order. Vendor data rates may vary.
- **Tunnel Virtual connection over the Underlay networks** – Provides a FIPS 140-2/3 compliant encrypted connection through one or more underlay networks.

EIS FEATURES (OPTIONAL)

- **Zero Trust Architecture (ZTA)** – ZTA is a feature offered under the EIS SD-WAN service. The Zero Trust model applies as no user, traffic source, or connected network above suspicion, regardless of location on or relative to the Agency Network. ZTA ensures authentication and authorization of all session-based network flows.
- **Virtual Trusted Internet Connection (vTIC)** – complies with the CISA TIC 3.0 program guidance and supports the Traditional (conventional) TIC, Branch Office, Cloud Service Provider, and Remote User use cases for high, medium, and low trust zones.
- **Network as a Service (NaaS)** – NaaS is a technical feature offered under the EIS SD-WAN service and is a Managed Network Service. NaaS virtualization continues to optimize the delivery of network functions; for example, as operational demands increase, functions can be scaled (e.g., bandwidth, capacity) and replicated across the environment. The NaaS virtualization will allow services to be optimally placed to meet demands or re-positioned to accommodate bottlenecks or outages in the underlying network fabric. NaaS is useful for agencies to operate

agency networks as a next-generation, professionally managed, and integrated infrastructure and enterprise service as a NaaS with central control and management.

- **Overlay Network (Control Plane)** – SD-WAN uses software-defined (SDN) concepts to distribute network traffic across a WAN to simplify the management and operation by decoupling the network hardware from its control mechanism, similar to virtualization. The SD-WAN follows configured policies to determine the most effective way to route application traffic automatically. The SD-WAN Controller provides centralized control to maintain connections across the control plane of the Edge/Gateway device, including configuration and activation of devices, IP address management, and establishing the policies applied to those devices. The SD-WAN Controller manages all of the Edge and Gateway devices on the network and interfaces with the management/orchestration components. These components are where the Service Orchestrator provides the service management of the SD-WAN service lifecycle, including service fulfillment, performance, assurance, usage, analytics, security, and policy.

EIS CAPABILITIES

- **Policy-Based Packet Forwarding** – Agency-defined policies are used to make application forwarding (or blocking) decisions for SD-WAN tunnels over each underlay.
- **Zero-Touch Provisioning of Site Equipment** – Universal CPE (uCPE) or virtualized edge router for SD-WAN connectivity and Agency-specific security functions (e.g., Firewall, IDS/IPS) required by the uCPE (utilizes EIS Managed Security Services (MSS).
- **Online Management and Control**—the ability to centrally define and update network monitoring, policy-setting, network segmentation, bandwidth allocation, or CIR for each application flow and other SD-WAN service profiles.

EIS FEATURES (OPTIONAL)

- **Online Management and Control (partial or full)** – the ability to control (define and update) aspects of the SD-WAN concerning application flows, creating/modifying application flow policies via a web portal or application programming interface (API). Available for either agency or co managed SD-WAN, depending on the agency approach.
- **Advanced Analytics and Reporting**- to define and configure SD-WAN network architecture for increased reliability and security for a large agency network, for example, "big data" analytics of real-time performance metrics of all SD-WAN connections.

Edge Devices – These devices are commonly located at the edge of the network and initiate and terminate secure overlay connections (e.g., IP-security (IPSec) or Transport Layer Security (TLS) tunnels). The Service Related Equipment (SRE) requires SD-WAN software that enables service operations.

These edge devices receive the data packets and determine how those data packets are handled and routed according to routing information, applicable policies, service attributes, etc. Network Function Virtualization (NFV) policy enforcement (i.e., firewalling, Network Access Control (NAC), TLS break and inspect, IDS/IPS, DLP, etc.), which are applied to some vendor Edge devices to ensure security policies are applied appropriately.

5.2 SD-WAN PRICING COMPONENTS

The price structure for SD-WAN is on an Individual Case Basis (ICB) service requiring specific details on agency requirements. EIS Contract Section B.2.8.10.1 sets forth the applicable Price Tables and Pricing Instruction Tables for SD-WAN. The Pricing Instruction Tables list all defined CLINS for the service. Users of this Guide should refer directly to EIS Contract B.2.8.10 to ensure they have the most up-to-date version of those Tables. The price structure for SD-WAN services consists of the components shown in Table 2 and Figure 3 on the next page.

TABLE 2: SDWANS PRICING COMPONENTS

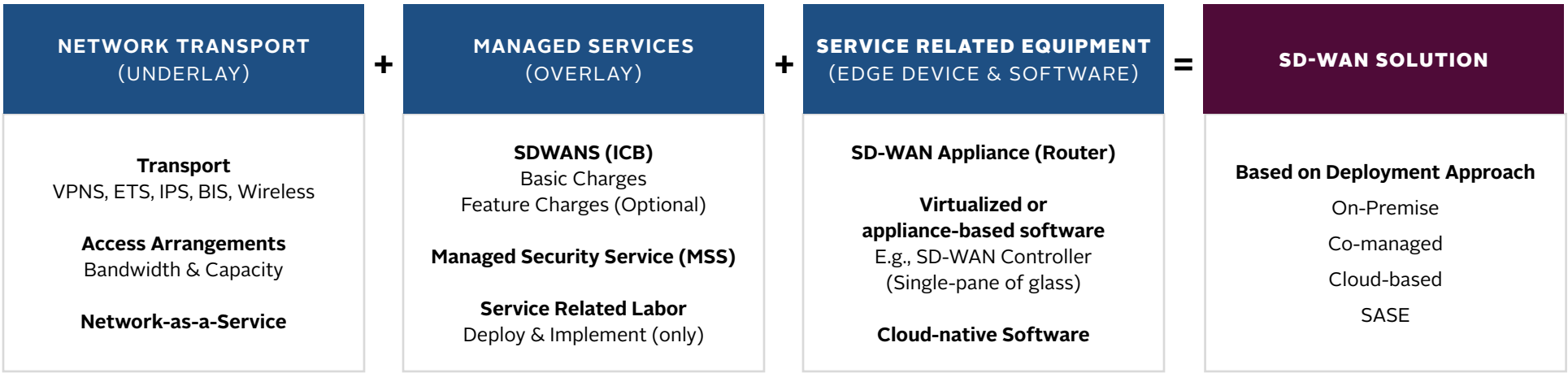
SD-WAN Pricing Components	
COMPONENT	**CHARGING UNIT**
Basic Charges: Policy, Design, Engineering, Management and Control	ICB
Feature Charges	ICB – for each Feature

The following EIS services support an SD-WAN solution.

- Access Arrangements (AA)
- Data Transport services (VPNS, ETS, IPS, BIS, etc.)
- Service Related Equipment (SRE)
- Managed Network Services (MNS)
- Managed Security Services (MSS)
- Network-as-a-Service (NaaS)

SD-WAN Service (SDWANS) is an overlay service on top of the agency data transport networks or underlay. Agencies coordinate with their provider to develop the specifics of each component. Not all components listed are in use, and incorporating other services fully develops the specific deployment approach. The figure below shows an example of how the pricing components combine to produce the total cost for the service.

FIGURE 3 SD-WAN FORMULA

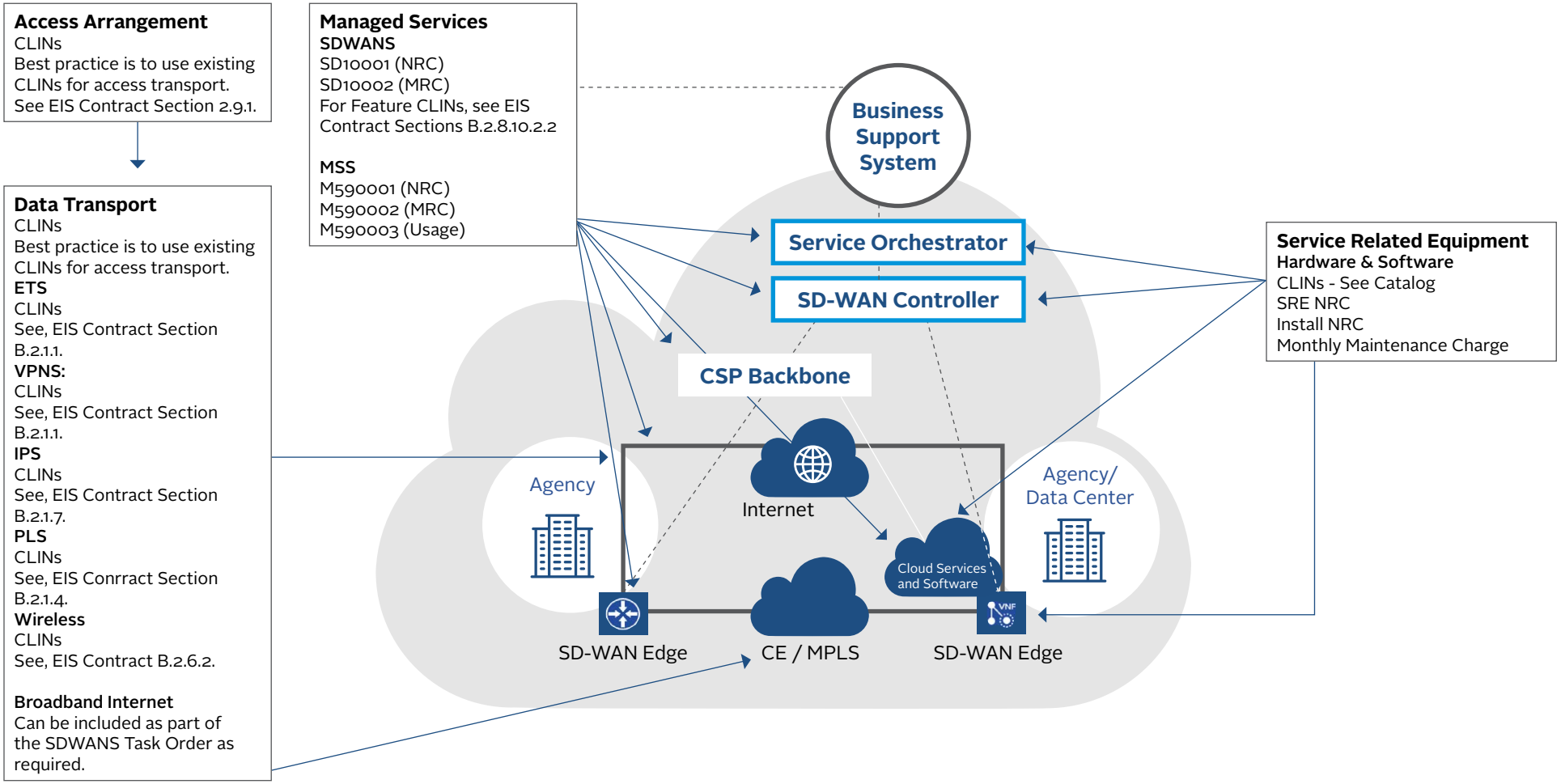


The EIS SD-WAN service offering includes optional CLINs for agencies that want to include the following in their SD-WAN solution:

- Network-as-a-Service (NaaS)
- Zero Trust Architecture
- Virtual Trust Internet Connection (vTIC)
- Advanced Analytics and Reporting

Using an SD-WAN Task Order Unique (TUC) Contract Line Item (CLIN) to further customize the solution to meet agency-specific needs.

FIGURE 4 EIS SD-WAN SERVICE OFFERING AND SUPPORTING SERVICES



6. References and Other Sources of Information

For additional EIS information and tools, visit the EIS Resources Listing.

For guidance on transitioning to EIS, please visit EIS Transition Resources.

For more information on CLINs for EIS services, see the CLIN list at: EIS Public Pricer.

For more technical details and information on SDWANS, please refer to Section C.2.8.10 of the EIS contract; for pricing details, please refer to **Section B.2.8.10**.

Please visit the EIS Contractors' Portal for information on specific contractor offerings for SDWANS.

Please see the EIS Pricing Tool & Guide for additional help in pricing this service.

For more information on the EIS services referenced above, please refer to the EIS contract sections listed below:

- For Access Arrangements, see EIS Contract Section C.2.9 (technical details) and Section B.2.9 (pricing details).
- For Ethernet Transport Service, see EIS Contract Section C.2.1.2 (technical details) and Section B.2.1.2 (pricing details).
- For Virtual Private Network Service, see EIS Contract Section C.2.1.1 (technical details) and Section B.2.1.1 (pricing details).
- For Internet Protocol Service, see EIS Contract Section C.2.1.7 (technical details) and Section B.2.1.7 (pricing details).
- For Private Line Service, see EIS Contract Section C.2.14 (technical details) and Section B.2.1.4 (pricing details).
- For Wireless Service, see EIS Contract Section C.2.6 (technical details) and Section B.2.6 (pricing details).
- For Service Related Equipment, see EIS Contract Section C.2.10 (technical details) and Section B.2.10 (pricing details).
- For Service Related Labor, see EIS Contract Section C.2.11 (technical details) and Section B.2.11 (pricing details).
- For Managed Network Service, see EIS Contract Section C.2.8.1 (technical details) and Section B.2.8.1 (pricing details).
- For Managed Security Service, see EIS Contract Section C.2.8.5 (technical details) and
- B.2.8.5 (pricing details).

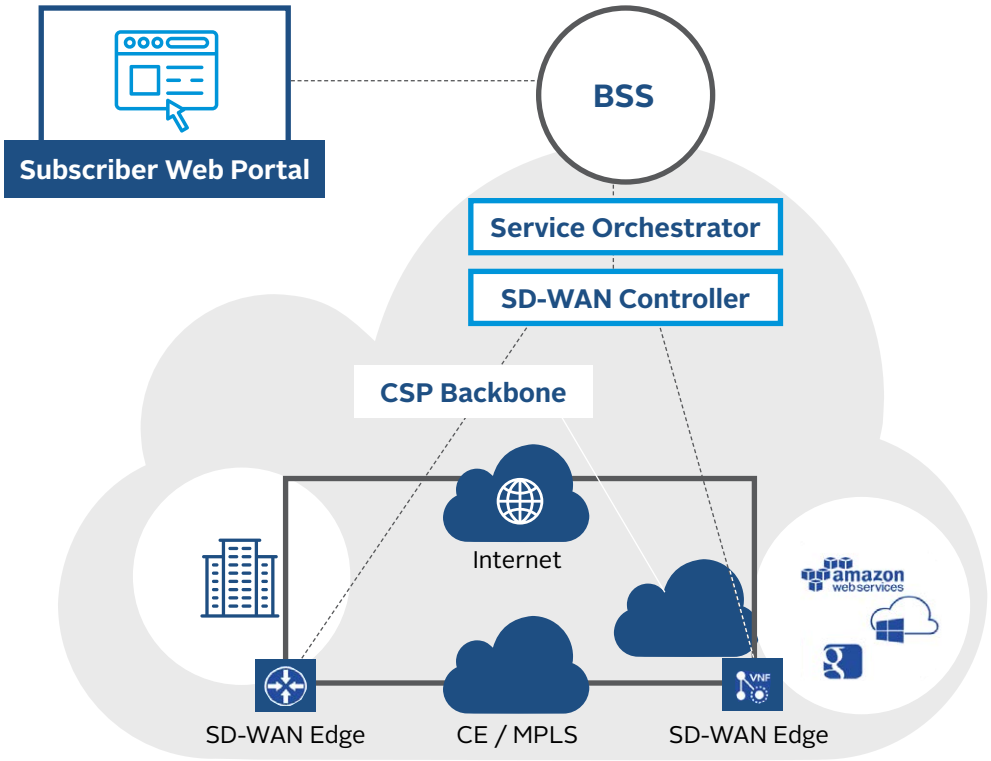
MEF, *Understanding SD-WAN Managed Services: Service Components, MEF LSO Reference Architecture and Use Cases*, July 2017.

MEF, *MEF 70: SD-WAN Service Attributes and Services*, July 2019. MEF Presentation, "MEF SD-WAN Services (MEF 70)"

MEF 0.2 SD-WAN Service Attributes and Service Framework

https://www.mef.net/resources/mef-70-2-sd-wan-service-attributes-and-service-framework/

FIGURE 5 MEF SD-WAN



Appendix 1: Updates to the MEF SD-WAN Reference Architecture

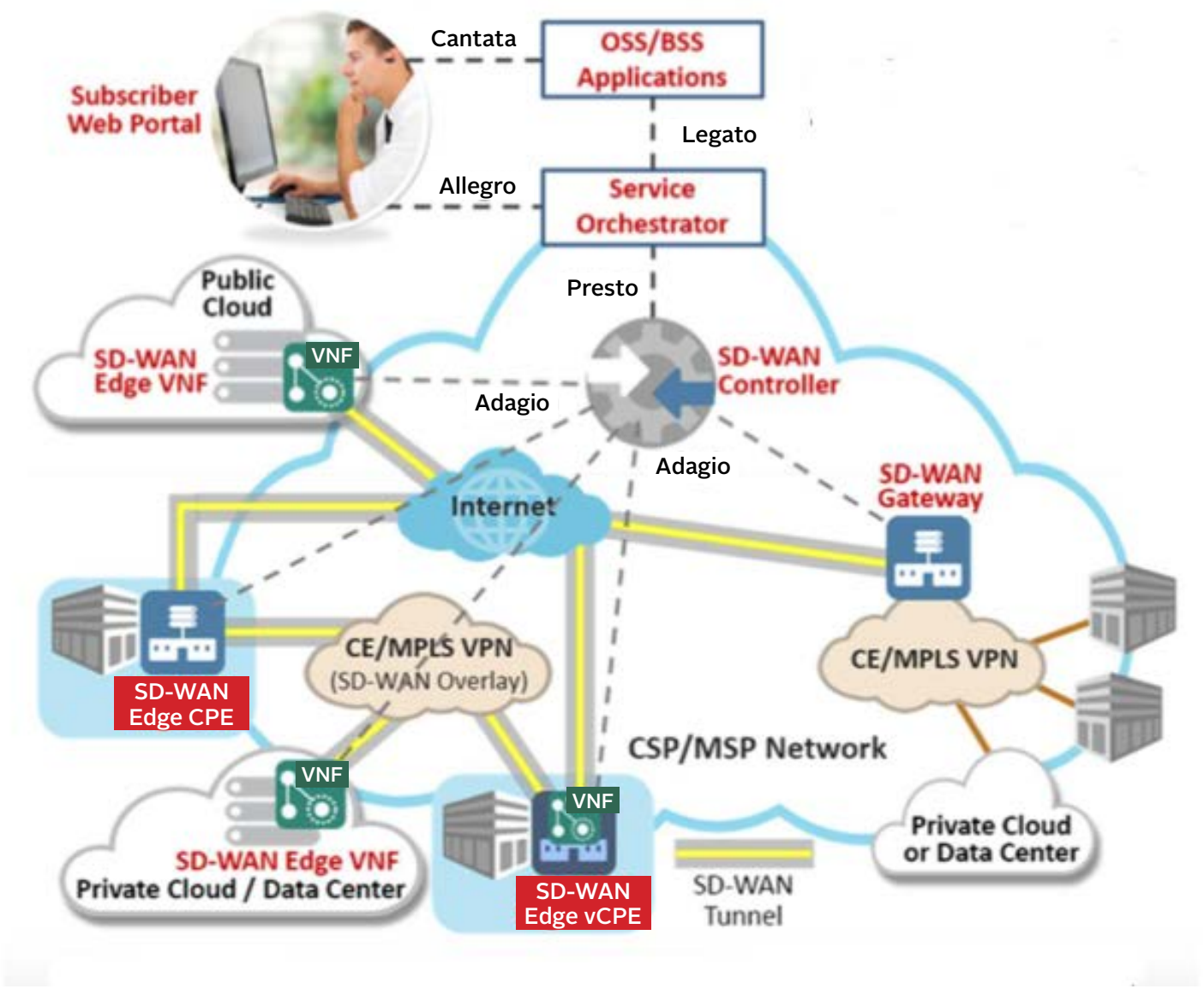
The following list represents the major changes in MEF 70.2 from the previous version, MEF 70.1:

- The UCS Billing Method Service Attribute removed Other as a possible value.
- Removed the SWVC Service Uptime Service Attribute.
- Removed the requirement that every Policy includes the same set of Policy Criteria and added/modified text in each Policy Criterion to define behavior when a Policy does not include the Policy Criterion.
- New SD-WAN UNI Service Attributes: SD-WAN UNI Availability Objective and SD-WAN UNI Mean Time To Repair Objective.
- New SWVC End Point Network Address Translation Service Attribute.
- Enhanced the PERFORMANCE Ingress Policy Criterion to include ceiling and remediation parameters values.
- New SWVC Service Attribute: SWVC Service Objectives Reporting Periods Service Attribute.
- Introduced Rate Limiter as a new “key concept” in section 7.15.
- Added new SWVC Service Attribute: SWVC List of Rate Limiters and modified the BANDWIDTH Policy Criterion to allow specification of a named Rate Limiter.
- Changed how Application Flows can share bandwidth. They use named Rate Limiters instead of belonging to the same Application Flow Specification Group.
- Added new Appendix with examples of the PERFORMANCE Policy Criterion (Appendix C).
- Included informative text in section 12 about UCS Service Attributes of which the SDWAN Service Provider must be aware.
- Added new SWVC Service Attribute: SWVC List of Application Flow Business.

Appendix 2: MEF 70 SD-WAN Reference Architecture

MEF has presented a reference architecture for SD-WAN. Figure 2 below provides MEF's illustration of that architecture, followed by a summary of its essential components.

FIGURE 6 SD-WAN REFERENCE ARCHITECTURE[11]



The reference architecture for SD-WAN includes the following basic components:[12]

- SD-WAN Edge
- SD-WAN Gateway
- SD-WAN Controller
- Service Orchestrator
- Subscriber Web Portal

The described components are below.

SD-WAN Edge: These devices[13] are located at the "edge" or periphery of the SD-WAN network and serve to initiate and terminate the FIPS 140-2/3 compliant encrypted connections that comprise the basic transport links of the virtual overlay network. They perform this function over the many different types of wired or wireless underlay networks that are compatible with SD-WAN. Edge devices also measure QoS performance in real-time, apply the selected QoS, security, and business policies to different data flows, and route them accordingly over the best- matching network underlay and overlay. In other words, Edges receive data packets from the transport network and determine how those data packets are handled and routed according to routing information, applicable policies, service attributes,[14] etc. Edges are part of the SD-WAN service provider's network but are commonly located at the customer's premises when it is a physical network function.

SD-WAN Gateway: This is essentially a variant of an SD-WAN Edge that also enables the connection of SD-WAN sites to other sites interconnected via alternative VPN technologies, *e.g.*, MPLS or Carrier Ethernet VPNs. While the gateway function permits intercommunication between the two VPNs, it isn't possible to extend SD-WAN characteristics such as application-driven packet forwarding into the VPNs that are beyond the boundaries of the SD-WAN itself.

SD-WAN Controller: An SD-WAN network has only one Controller, which is responsible for managing all of the Edge and Gateway devices on the network. Device management includes configuration and activation of devices, IP address management, and establishing the policies applied to those devices. The SD-WAN controller maintains connections to all SD-WAN Edges and SD-WAN Gateways to identify the operational state of SD-WAN paths across different WANs and retrieves QoS performance metrics for each SD-WAN path.

Service Orchestrator: "The Service Orchestrator provides the service management of the SD-WAN service lifecycle, including service fulfillment, performance, control, assurance, usage, analytics, security and policy." The SD-WAN Controller and Service Orchestrator functions combine in some providers' implementations of SD-WAN.

Subscriber Web Portal or API: This provides the "dashboard" interface for the centralized management and control of the SD-WAN. Providing a web portal is typical for a Managed Service implementation of SD-WAN, whereas using an API is typical for DIY implementation. Both versions serve the same purpose: allowing appropriately credentialed users to engage in network monitoring, management, or service modifications, such as establishing different QoS, security, or business policies.

Resource References:

- MEF, *Understanding SD-WAN Managed Services: Service Components, MEF LSO Reference Architecture and Use Cases*, July 2017.
- MEF, *MEF 70: SD-WAN Service Attributes and Services*, July 2019. MEF Presentation, "MEF SD-WAN Services (MEF 70)".
- MEF 70.2 SD-WAN Service Attributes and Service Framework.
- In MEF 70.1, the value of the SWVC List of Security Policies Service Attribute (section 9.10) could be None, in MEF 70.2, that value representation is an empty list.
- Changed the effect of INTERNET-BREAKOUT=Enabled. Forwarding IP Packets in the Application Flow to Internet destinations or to UNI destinations based on their IP Address. In MEF 70.1, they are forwarded to Internet destinations.
- Changed the value of ALLOWED-DESTINATION-ZONES to allow an empty list. This change works with INTERNET-BREAKOUT=Enabled to achieve behavior compatible with MEF 70.1 (see previous bullet).
- The BLOCK-SOURCE Egress Policy Criterion changed to EGRESS-BLOCK with values Allow and Discard.

Appendix 3: EIS Services Used in Conjunction with SD-WAN: Pricing

This section provides an overview of the price structures of the existing EIS services used in conjunction with either a managed SDWANS or a DIY SD-WAN solution. Agencies should refer directly to the relevant EIS contract sections (cited below) for the most up-to-date information on how those services are priced and their applicable CLINs.

6.1.1 ACCESS ARRANGEMENTS

AA – the price structure for AA includes the following elements: (1) non-recurring charge, (2) monthly recurring charge, (3) usage charges, and (4) feature charges. The following types of defined access for EIS: wireline access, Ethernet access, cable access, Fiber-to-the-Premises, and wireless access. AA pricing formats and instructions tables are found in EIS Contract Sections B.2.9.1.1, B.2.9.1.1.1, B.2.9.1.2, B.2.9.1.3, B.2.9.1.4, B.2.9.1.5, B.2.9.1.6, B.2.9.1.7, B.2.9.1.8, B.2.9.1.9, B.2.9.1.10, B.2.9.1.11, and B.2.9.1.12.

6.1.2 DATA TRANSPORT SERVICES

Broadband Internet Access –GSA is working with EIS vendors to develop an EIS Contract Mod for this service offering. It is a cost-effective primary transport option for many agencies to use with SDWANs and DIY SD-WAN solutions.

Ethernet Transport Service – the price structure for ETS includes the following elements: (1) port price, (2) Ethernet Virtual Connection (EVC) price, and (3) features. ETS is available in two scenarios: E-LINE and E-LAN. E-LINE service requires two ports (point-to-point) with an EVC connecting them. The total price of E-LINE includes the sum of two ports, EVC, and any features. E-LAN requires two or more ports. The total price of E-LAN includes the sum of the ports and any features. ETS pricing format and instructions tables (for ports, EVC and features) are found in EIS Contract Sections B.2.1.2.2.1, B.2.1.2.2.2, B.2.1.2.3.1, B.2.1.2.3.2, B.2.1.2.4.1, B.2.1.2.4.2, B.2.1.2.5.1, and B.2.1.2.6.

Virtual Private Network Service - the price structure for VPNS includes the following elements: (1) transport charges, (2) transport with embedded access charges (optional), and (3) feature charges. Pricing for VPNS depends on a number of factors including the number of sites, bandwidth requirements, additional security services and type of access. VPNS pricing format and instructions tables found in EIS Contract Sections B.2.1.1.3.1, B.2.1.1.3.2, B.2.1.1.3.3, B.2.1.1.3.4, B.2.1.1.4.1, B.2.1.1.4.2, and B.2.1.1.5.

Internet Protocol Service – the price structure for IPS includes the following elements: (1) monthly recurring charge per port and (2) feature charges. IPS pricing format and instructions tables found in EIS Contract Sections B.2.1.7.3.1, B.2.1.7.3.2, B.2.1.7.4.1, and B.2.1.7.5.

Private Line Service – the transport prices for PLS depend on the locations of the points of presence (POPs) (*see*, EIS Contract Section B.2.1.4.1). PLS pricing format and instructions tables found in EIS Contract Sections B.2.1.4.1.1, B.2.1.4.1.2, B.2.1.4.1.3, B.2.1.4.1.4, B.2.1.4.1.5, B.2.1.4.2.1, B.2.1.4.2.2, and B.2.1.4.3.

Wireless Service – the price structure for wireless service includes the following elements: (1) non-recurring charges, (2) monthly recurring charges, and (3) usage charges. Wireless Service mobile data pricing format and instructions tables found in EIS Contract Sections B.2.6.2.1, B.2.6.2.2, B.2.6.3.1, B.2.6.3.2, B.2.6.7.3.1, B.2.6.7.3.2, and B.2.6.7.4.

6.1.3 EQUIPMENT AND LABOR

SRE – refers to separately identifiable and separately priced hardware, firmware, and software components, along with installation, maintenance, relocation, and/or removal. All equipment (hardware, firmware, and software) needed on the contractor's side of the demarcation point to provide a service is part of the EIS service, and pricing is not separate under SRE. SRE utilizes catalog pricing. The price structure for SRE includes the following elements: (1) initial installation (NRC), (2) inside moves (NRC), (3) on-site modification/upgrade (NRC), (4) monthly maintenance charge, and (5) monthly installment charge. EIS Contract Section B.2.10.3.1 provides pricing elements with each SRE included in a contractor's SRE Catalog. Contractors can request additional pricing elements as desired.

SRL – labor is either time and materials or fixed price basis. SRL pricing format and instructions tables found in EIS Contract Sections B.2.11.7.1, B.2.11.7.2, and B.2.11.7.3.

Glossary

Acronym	Description
AA	Access Arrangements
API	Application Programming Interface
ATP	Advanced Threat Protection
BIS	Broadband Internet Service
CASB	Cloud Access Security Broker
CLIN	Contract Line Item Number
CPE	Customer Premises Equipment
DIA	Dedicated Internet Access
DNSSEC	Domain Name System Security
DTLS	Datagram Transport Layer Security
EIS	Enterprise Infrastructure Solutions
ETC	Ethernet Transport Service
FWaaS	Firewall-as-a-Service
GSA	General Services Administration
HQ	Headquarters
ICB	Individual Case Basis
IPS	Intrusion Prevention System
IPS	Internet Protocol Service
MEF	Metro Ethernet Forum
MNS	Managed Network Services
MPLS	Multiprotocol Label Switching
MSS	Managed Security Services
MWS	Managed Wireless Service
NaaS	Network-as-a-Service
NAC	Network Access Control
NGFW	Next-Generation Firewall
QoS	Quality of Service
SaaS	Software-as-a-Service

Acronym	Description
SASE	Secure Access Service Edge
SD-WAN	Software Defined-Wide Area Network
SDWANS	Software Defined Wide Area Network Service
SRE	Service Related Equipment
SSL	Secure Socket Layer
SWG	Secure Web Gateway
TIC	Trusted Internet Connection
TLS	Transport Layer Security
TUC	Task Order Unique
VPN	Virtual Private Network
VPNS	Virtual Private Network Service
WAN	Wide Area Network
ZTA	Zero Trust Architecture
ZTNA	Zero Trust Network Access

Contributors

Organization	Introduction	Slip Sheet	White Paper	Use Cases	How To Get	FAQ/Lessons Learned
General Services Administration (GSA)	X			X	X	
JPI Solutions (JPI)	X			X	X	