SD-WAN OVERVIEW AND ORDERING GUIDE

Enterprise Infrastructure Solutions (EIS)

SD-WAN Overview and Ordering Guide

Issued by:
General Services Administration
Office of Telecommunications Services
1800 F St NW
Washington, DC 20405

Version 2.0

August 2020

Table of Contents

Figures

Tables

SD-WAN OVERVIEW AND ORDERING GUIDE

1 Introduction

This SD-WAN Overview and Ordering Guide ("Guide") is intended to assist Federal agency telecommunications customers seeking to implement Software-Defined Wide Area Network ("SD-WAN") technologies under Enterprise Infrastructure Solutions ("EIS") contract task orders. The primary target audience of the Guide is Federal agency customers considering whether and how to incorporate SD-WAN into their telecommunications networks. This Guide incorporates information from the industry's first voluntary SD-WAN standard – *SD-WAN Service Attributes and Services* (MEF 70) – published by the MEF Forum in July 2019 (hereafter "MEF 70"). SD-WAN is a virtual WAN network architecture that utilizes various data transport technologies and a centralized control function to securely and intelligently connect users to applications. Unlike traditional WAN, SD-WAN de-couples the transport service[1] from its applications and software control function,[2] resulting in a more agile, reliable and cost-effective network architecture. Because the software control operates as a separate plane from the underlying network transport functions, SD-WAN acts as an overlay network to monitor, manage, and optimize the use of that transport. Regarding data transport, SD-WAN permits a Federal agency to combine and integrate multiple data transport technologies – which can include Multiprotocol Label Switching ("MPLS"), carrier Ethernet ("CE"), public Internet, fixed and mobile wireless, and satellite-based services. Regarding the applications and control function, SD-WAN relies on pervasive software control working in concert with intelligent network "edge" devices to provide network-wide dynamic traffic routing and prioritization functionality, policy-setting capabilities, and quicker more efficient network deployments and configurations.

Certain market drivers are pushing enterprises to adopt SD-WAN, including the following:

1) High-cost legacy networks (most frequently, 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 to have more centralized network monitoring and management capabilities;
3) Expense and inefficiency caused by backhaul of traffic from branch/remote locations to headquarters or centralized data centers, often to meet cybersecurity requirements; and
4) Overcoming cybersecurity vulnerabilities/challenges that have made the traditional "perimeter" network defense strategy inadequate.

---

[1] The WAN transport service is commonly referred to as the "data forwarding plane."

[2] The applications and control function is commonly referred to as the "control plane."

Key findings and conclusions set forth in this Guide include:

- SD-WAN is a major advance in wide-area networking, that nearly every Federal agency will need to consider adopting and most will eventually find to be a compelling option.
- SD-WAN is ideal for a Federal agency looking to rely more heavily on cloud-based applications, while avoiding 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.
- A Federal Agency may want to evaluate whether a Managed Service option or Do-It Yourself ("DIY") option best meets its needs, by evaluating the agency's IT resources and the complexity of its networking needs. Some Federal agencies may find that a Co-Managed SD-WAN provides the optimum balance, by leaving 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. Currently, SD-WAN is a Managed Service under the EIS Contract. *See*, EIS Contract Sections B.2.8.10 and C.2.8.10 (SDWANS).

Category: Managed Services.

Complementary Services Needed: In order to use SDWANS, the agency would need EIS Transport services, such as VPNS, ETS, IPS, and Broadband Internet Service ("BIS") provided by SDWANs.

Definitions: Please see the EIS Acroynyms 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.

2 Overview of SD-WAN Technology

A Wide Area Network (WAN) is a communications network that spans a large geographic region and connects networks/users in one location to networks/users in other locations. Traditionally, WANs often have been implemented using a private high-speed network in a hub and spoke architecture – with data centers at the hub(s) and the spokes extending to branch offices and other user locations (which can be tens, hundreds, or thousands of miles from a hub). Notably, traditional WANS will often apply cybersecurity tools at a central hub, thus necessitating backhaul of all traffic into that hub for verification prior to reaching its final destination. Most of the network control in a traditional WAN is decentralized, with routers at each node independently making decisions about their traffic from a local perspective. These WAN networks were originally designed to support relatively predictable and unvarying telecommunications requirements, and have worked well (or at least adequately, in most cases) for that purpose. However, traditional WAN networks are becoming increasingly unsuited for keeping up with today's highly dynamic demands for bandwidth and connectivity, driven by video, mobile data, and other data-intensive and cloud-based applications.[3]

SD-WAN is now seen throughout the industry as a key 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. However, SD-WAN is still an evolving and fluid technology, and its standardization is a work-in-progress. The best available industry source for a SD-WAN standard is MEF 70, recently issued in July 2019,[4] the industry's first version of an SD-WAN service definition standard.[5] MEF 70 contains the following diagram of an SD-WAN network architecture.

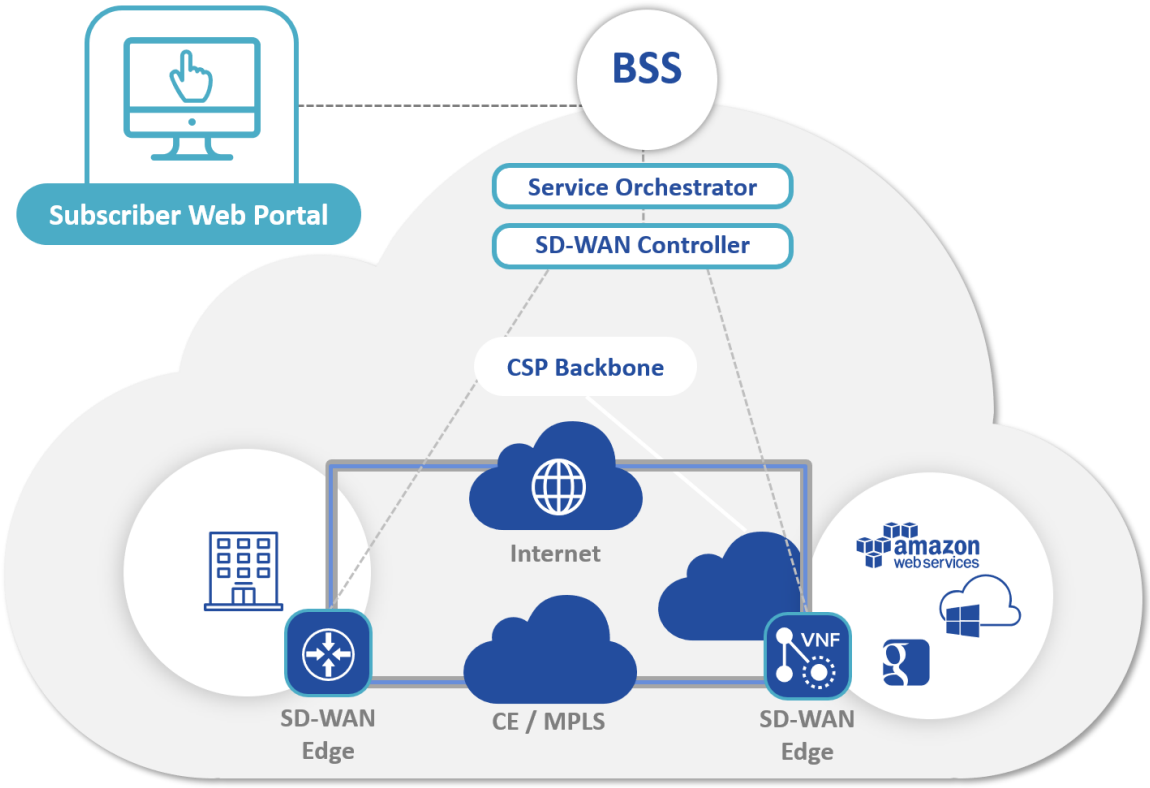
---

[3] For example, CTIA reports that wireless mobile data grew by 82% in just one year (2018), and has increased 73-fold since 2010. See CTIA 2019 Annual Survey Highlights, https://www.ctia.org/news/2019-annual-survey-highlights .

[4] *See* https://www.mef.net/about-mef MEF describes itself therein as an "industry association of 200+ member companies, MEF is the driving force enabling agile, assured, and orchestrated communication services that empower users with the dynamic performance and security required to thrive in the digital economy."

[5] *See* https://www.mef.net/mef-3-0-sd-wan MEF places MEF 70 within its MEF 3.0 Transformational Global Services Framework, "for defining, delivering, and certifying assured communications services orchestrated across a global ecosystem of automated networks." See https://www.mef.net/mef30/overview

Figure 1: Illustrative SD-WAN Deployment[6]



In brief, Figure 1 illustrates the separation of the control plane (consisting of the upper elements, Subscriber Web Portal, Service Orchestrator, and SD-WAN Controller) vs. the data forwarding plane, where SD-WAN Edge functions are connecting agency locations to the cloud via two transport options: (1) a traditional Carrier Ethernet or MPLS network and (2) the public Internet. All of these elements will be described below.

2.1 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

[6] This is an illustration of a typical SD-WAN deployment, under a Managed service scenario. (Reproduced with permission of the MEF Forum.) Source: MEF, *MEF SD-WAN Services (MEF 70)* presentation (Undated), at page 5. Available from: https://www.mef.net/resources/White-Papers Additional scenarios and a reference architecture are supplied below.

[7] *See* MEF 70, Section 5.2. See also, MEF, *Understanding SD-WAN Managed Services: Service Components, MEF LSO Reference Architecture and Use Cases*, July 2017 (hereafter, "*Understanding SD-WAN*"), pp. 5-6. Available from: https://www.mef.net/resources/White-Papers)

that utilizes virtual connections riding on that existing transport. Typically, SD-WAN will use IPSec tunnels[8] 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:** QoS is measured in real-time on key parameters (latency, packet loss, etc.), with the results used to ensure that the performance level specified by the network manager is being achieved.
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 will utilize. (This is a specific instance of the "Policy-based Packet Forwarding" characteristic discussed below.)
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 availability of connectivity.
6. **Policy-based Packet Forwarding:** SD-WANs can apply customized networking policies to different types of packet flows. This means users can choose their desired quality-of-service, security, and/or business policy and their traffic will then flow 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"). Network monitoring and administration can be performed in real-time, with different levels of access and control granted to different roles (*e.g.*, service provider, network administrator, network user). A novel aspect of this centralized management is that SD-WAN enables "zero touch provisioning" of Customer Premises Equipment ("CPE"): when new SD-WAN CPE is powered up and connected, it can retrieve its configuration and policies without needing to send a service provider installer to the site.

---

[8] IPSec is a standard secure network protocol suite that can encrypt and authenticate data packets. A SD-WAN service provider typically builds point-to-point paths called Tunnel Virtual Connections ("TVCs") across the data transport network. Each TVC is built using a well-defined set of characteristics. Those characteristics can include the following: (i) whether the TVC is public or private, depending on the type of transport on which it is built, (ii) encrypted or unencrypted, etc. See MEF 70, pp. 14-15.

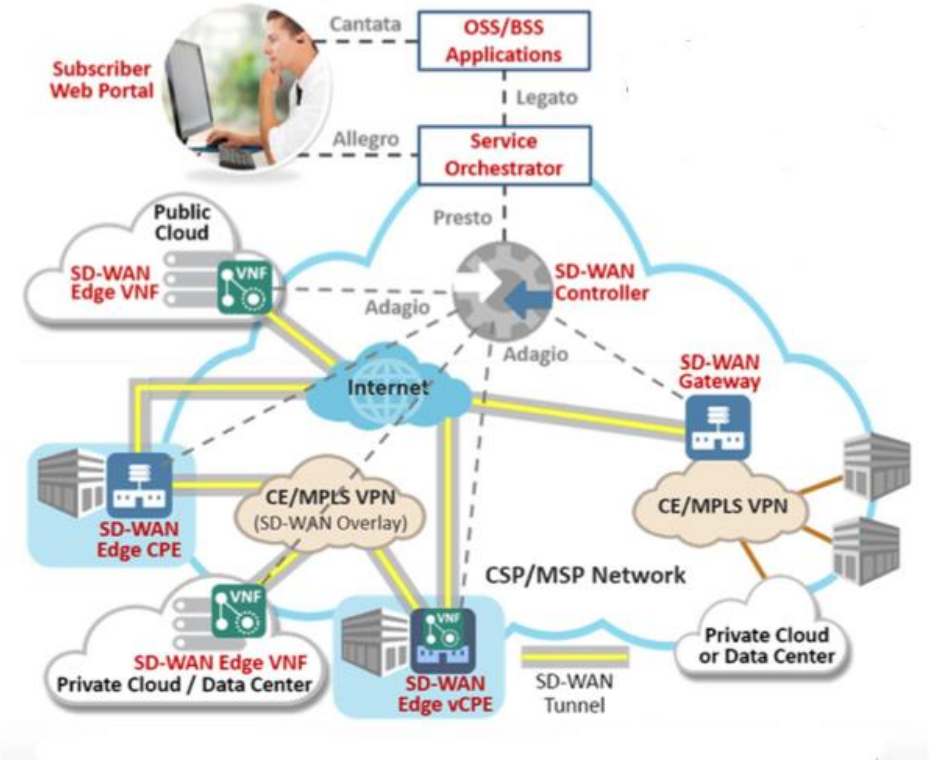
[9] DIA provides a dedicated link to an Internet backbone network, rather than one shared among multiple customers that may be subject to traffic congestion and slow-downs. DIA typically is more expensive than best-effort broadband, but provides a guaranteed level of service quality (bandwidth) backed by a Service Level Agreement ("SLA").

[10] When a site has two or more WAN connections and each WAN uses a different WAN technology, *e.g.*, Internet and MPLS VPN, it is referred to as a "hybrid WAN."

2.2 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 2: 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

These components are described 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

[11] Source: *Understanding SD-WAN*, p. 12 (Figure 9). (Reproduced with permission of the MEF Forum). Note that this figure contains not only the various SD-WAN components, but secondarily also identifies the standardized interfaces between functions of the MEF's Lifecycle Service Orchestration ("LSO") construct (Cantata, Allegro, Legato, etc.). For more details on these interfaces, *see* MEF 55, *Lifecycle Service Orchestration (LSO): Reference Architecture and Framework*, March 2016.

[12] *See Understanding SD-WAN*, pp. 7-9. Note that the MEF 70 document itself does not supply a reference architecture.

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 network 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 should be 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 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. he 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 may be combined in some provider's implementations of SD-WAN.

Subscriber Web Portal or API: This provides the "dashboard" interface for the centralized management and control of the SD-WAN. A web portal is typically provided for a Managed Service implementation of SD-WAN, whereas an API is typically used 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.

---

[13] In reality, the "Edge" is a set of functions that can be performed by a physical CPE device, or implemented as a software-based virtual network function ("VNF") running on a virtual CPE. See MEF 70 at Section 6.2.

[14] "Service attributes" refers to capturing specific information that is agreed on between the SD-WAN service provider and subscriber and describes some aspect of service behavior, such as service uptime, application of flow objectives, etc.

3 Why SD-WAN?

This section reviews the marketplace factors that are driving enterprises to adopt SD-WAN, the benefits and potential risks of the technology, and some examples of how a Federal agency could use SD-WAN to improve its delivery of network capabilities.

3.1 Market Drivers for SD-WAN Adoption

Many private sector enterprises and some forward-thinking public sector agencies[15] have been turning to SD-WAN as a new and 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 to have 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 seen as driving SD-WAN adoption is the existence of a de-centralized, disaggregated IT/telecom infrastructure with no centralized management or monitoring capabilities.

A fourth common driver of SD-WAN adoption is delayed/slow market roll-out or limited location placement due to a dependence on carrier provisioning of lines or circuits.

A fifth common reason given 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.

Other common drivers to SD-WAN as identified by enterprises include overcoming cybersecurity vulnerabilities/challenges and increasing demand for cloud-based applications. As explained further below, routing cloud-based services traffic through a common data center, as typically occurs in a traditional WAN, degrades performance and unnecessarily consumes

---

[15] One example is California's Monterey County, which has been deploying SD-WAN to about one-quarter of its 120 locations, allowing it to reduce costs while maintaining service quality by substituting Internet transport for MPLS circuits. See State Tech Magazine, "SD-WAN Technology vs. MPLS: Cutting Costs on the Road to Digital Transformation" (6/26/2018), https://statetechmagazine.com/article/2018/06/sd-wan-technology-vs-mpls-cutting-costs-road-digital-transformation-perfcon

[16] QSI, *Report on SD-WAN Industry Use and Test Cases* (5/21/2019), p. 4 and Attachment 1. Similar SD-WAN deployment drivers are seen in other market studies, *see, e.g.*, Jim Hodges, Heavy Reading Reports, "SD-WAN Implementation & Differentiation Layer Strategies" (February 2017), produced for Juniper Networks, https://www.juniper.net/assets/us/en/local/pdf/whitepapers/2000666-en.pdf . *See* also the MEF Webinar "Standardized MEF 3.0 SD-WAN Services: Aligning the Industry" (05/22/1019). Available from: https://www.brighttalk.com/webcast/12779/357538?utm_source=MEF&utm_medium=brighttalk&utm_campaign=357538%20

bandwidth. SD-WAN can allow for direct routing to/from cloud-based services, thereby increasing networking efficiency, without compromising cybersecurity.

3.2 SD-WAN Benefits and Risks

SD-WAN is now seen in the industry as a major innovation that can improve WANs' performance and solve the most common problems faced 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, for some sites and applications, agencies can replace expensive, high-performance MPLS circuits with cheaper, best-effort broadband Internet or wireless 4G LTE connectivity.[17] The cost savings can be 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] In addition, 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.
- In similar fashion, the "zero-touch" capability of SD-WAN allows agencies to undertake fast and simplified set-up/take-down of network "edge" locations. This can be a compelling advantage for agencies that experience rapid turnover of remote locations needing access to their network. Combined with 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.
- By making use of multiple data transport technologies – which can use physically-distinct facilities for diversity – in a blended, seamless fashion via its dynamic policy control capabilities, SD-WAN can greatly improve network resiliency as well as overall network uptime.

---

[17] The industry also anticipates that fifth-generation "5G" wireless services will also play an important role in the underlying connectivity for SD-WANs as those services are deployed.

[18] Given the wide variation in actual network architectures and their served demand, it is not feasible to provide meaningful price comparisons on a generalized basis.

Among the highest-priority goals when deploying SD-WAN will be to ensure that Federal cybersecurity requirements will be met, not only upon initial adoption but on a continuous, ongoing basis. Those requirements are prescribed by the FISMA 2014 law[19] and its implementation in the NIST guidelines on cybersecurity. With respect to use of cloud services, the FedRAMP website provides detailed information about how a Federal agency can select a Cloud Service Provider ("CSP") who is FedRAMP certified (or who can become certified).[20] The site also explains FedRAMP recommendations and best practices for Federal agencies' ongoing cybersecurity risk management with respect to CSPs.[21] In addition, the longstanding Trusted Internet Connections ("TIC") initiative, designed to ensure the security of Federal networks' external connections to the Internet, is undergoing important revisions to adapt to cloud-based and SD-WAN technologies and architectures. Until now, TIC has required Federal agency traffic to flow through a limited number of physical TIC access points where cybersecurity controls can be applied. In September 2019, the Office of Management and Budget ("OMB") issued a Memorandum rescinding those requirements, replacing them with a process by which agencies can determine their preferred security controls from a suite of predefined TIC Use Case(s).[22] The Memorandum identified new TIC Use Cases compatible with the most popular cloud solutions (*e.g.*, IaaS, SaaS, PaaS) and SD-WAN (as well as retaining the traditional TIC solution as a default). It also established a new collaborative process for iterative development of these and additional TIC Use Cases over time, and requires agencies to update their own network boundary policies to conform to the Memorandum within one year.[23] Federal agencies will need to closely monitor the evolution of the "TIC 3.0" framework and ensure that their SD-WAN implementations comply with it.

From an implementation perspective, SD-WAN also has an important advantage. As an overlay network, SD-WAN can be adopted gradually over time, site-by-site, rather than requiring a flash-cut transition to a new network technology. By choosing a "go-slow" approach, an agency can greatly reduce any perceived risks from its move to SD-WAN.

SD-WAN is generally considered in the industry as a robust, highly adaptive technology. However, one downside cited by some critics is that SD-WAN requires additional "overhead" bandwidth to support its greater functionality. Under certain relatively extreme scenarios,[24] the percentage of overall bandwidth consumed by overhead could be substantial and represent a drag on network performance and overall cost. Under normal operating conditions however, SD-WAN's overhead bandwidth requirements tend to be relatively small, and can be controlled (with tradeoffs) by changing network QoS and security policies. To guard against unwelcome surprises in this area, federal agencies should require that vendor proposals for SD-WAN

---

19 Federal Information Security Modernization Act of 2014, Public Law No: 113-283 (12/18/2014).

20 *See* https://www.fedramp.gov/federal-agencies/

21 *See id.* and the FedRAMP's Agency Authorization Playbook, at https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf

22 OMB, Memorandum for Heads of Executive Departments and Agencies: Update to the Trusted Internet Connections (TIC) Initiative, M-19-26, released 9/12/2019; https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf

23 *Id.*, p. 3.

24 For example, overheads can exceed 100% on traffic with very small packet sizes, or under policies that rely on active transport redundancy to ensure the highest level of QoS for certain traffic.

solutions include estimates of their bandwidth overheads under realistic implementation scenarios for the agency.

Beyond that issue, SD-WAN's risks mainly arise from how it is implemented and in the transition from the embedded network. For example, if an enterprise fails to adequately assess its telecommunications needs (including its traffic profiles, performance requirements, and forecasted demand growth), it could choose an SD-WAN option (or underlying data transport technologies) that fail to match its actual needs. This could also occur if a pilot test isn't properly designed to reflect representative conditions. Federal agencies should heed that recommendation, and ensure that their solicitations for SD-WAN include well-defined testing criteria for purposes of evaluating the relative performance of vendors' proposed solutions. Another potential risk is becoming locked-in to a particular vendor's SD-WAN implementation, in part because vendor's SD-WAN controllers have proprietary characteristics and typically can't be integrated with other vendor's SD-WAN technology.[25]

The topic most-frequently raised with respect to SD-WAN risks is cybersecurity, in large part because of its heavy reliance on transport over the public Internet. While the unsecured nature of the public Internet must be recognized and addressed, the dynamic, policy-driven approach fundamental to SD-WAN goes a long way towards overcoming that challenge. 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"). When provided via a fully cloud-based security platform, security requirements can be applied consistently at every branch office and remote site.

3.3 Examples of How SD-WAN Could be Used

The experiences of private sector enterprises illustrate several ways in which a Federal agency could improve their 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 also among the highest-cost transport options, in part because they typically require a hub-and-spoke architecture in which all traffic must be back-hauled 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, and without back-hauling.
- **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 essentially real time, either through direct control of the SD-WAN central dashboard (in a DIY or co-managed arrangement) or via their vendor (in a Managed arrangement). Similarly, new agency

[25] *Id.*, p. 16.

branches and field locations can be connected in hours to minutes with two broadband internet connections and an "Edge" device without trained technicians, instead of it 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 securely access agency resources.
    - An agency could use SD-WAN to enable remote offices to securely connect to the agency's intranet.
    - An agency with a large number of 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 can give workers access to the same information and IT assets that they would have sitting at their desktops. Compared to traditional WANs, SD-WAN can do this more cheaply and flexibly.
    - SD-WAN could be used to enable authorized private and government partners to gain access, via a secured agency extranet, to agency applications and data.

4 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 is intended to serve 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 carefully consider its own circumstances, including its present and future telecommunications needs, budgetary and personnel resources, and the status of its existing network infrastructure.

Table 1: Checklist for Agency Consideration of SD-WAN Adoption

	YES	NO
1. Does your agency have (or can obtain) sufficient budgetary resources to start implementing an SD-WAN overlay?	☐	☐
2. Is use of public Internet and/or wireless transport options consistent with your agency's System Security Plan? (Take into account OMB'S TIC 3.0 security initiative.)	☐	☐
3. Is your agency free from other operational considerations (e.g., low latency requirements) that would deter or prevent it from using Internet or wireless transport? (Take into account 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 will be 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 might be mitigated by an SD-WAN solution that integrates additional transport options for purposes of route diversity, redundancy, and backup?	☐	☐
9. Does your agency experience significant turnover (additions/eliminations) of branch offices or other user locations that requires network personnel to go on-site to effect those changes?	☐	☐

If your agency can't satisfy the first two items on the checklist, that might disqualify SD-WAN from further consideration at this time.[26] However, if those baseline conditions are met, then saying "Yes" to any combination of the following seven factors – even to just one or two, if they resonate strongly for your agency – suggests that you should seriously consider adopting SD-WAN for your network. In that case, the next step should be to undertake an in-depth network assessment, covering both the existing network infrastructure and current demand profiles, plus forecasted changes in demand (taking into account cloud migration, data volume growth etc.) to better understand your agency's needs. This can be done internally or with the assistance of third-party consultants with the necessary expertise. Revisit the checklist with that information in hand – plus any additional considerations that are particularly important for your agency – before reaching a decision about whether to proceed.

[26] It is possible for an agency to eschew the use of public internet or wireless transport and still adopt SD-WAN with only MPLS (or another transport service, such as Ethernet E-Line, Private Line Service, etc.) as the transport underlayer. However, that choice would forego certain cost savings and efficiency benefits of the multimodal, integrated approach to transport that is a primary feature of SD-WAN.

5 SD-WAN Implementation

5.1 Is DIY or Managed Service the Best Fit for Your Agency?

Once it has become clear that SD-WAN may be beneficial for your agency to adopt, the next threshold question is whether a DIY or a Managed Service option provides the best fit.

In the commercial marketplace, Managed SD-WAN comes in many "flavors." On one end of the spectrum is fully "managed" SD-WAN service, which is a carrier-grade network offering that is completely managed by the network operator and delivered over a SD-WAN architecture on a turn-key basis. In the middle, Co-Managed solutions have the customer and service provider split responsibilities such as initial configuration, network monitoring, trouble ticketing, etc. On the other end of the spectrum is the fully DIY SD-WAN solution, wherein the customer's telecommunications/IT department(s) purchases the SD-WAN network software and hardware[27] from a vendor and takes full responsibility for installing, managing and maintaining it.

In May 2020, GSA released an EIS Contract Modification ("Mod") for a new optional service offering, Software Defined Wide Area Network Services ("SDWANS"). SDWANS allows EIS vendors to provide a managed SD-WAN solution to Federal agencies, with the flexibility to accommodate agencies' specific needs as well as changes in vendors' SD-WAN capabilities as the technology continues to evolve.

A separate EIS Contract Mod is being developed to add Broadband Internet Service ("BIS"), which will offer a cost-effective underlay network option for SDWANS.

The table below gives a high-level overview of the main tradeoffs between the DIY vs. Managed SD-WAN options along basic dimensions such as cost, performance, and security.

Table 2: Comparison of DIY vs. Managed Options for SD-WAN Solutions

Issue	Do-It-Yourself (DIY) Option	Managed Options
Speed of Initial Deployment	Depends on capabilities and resources of internal staff; assistance from the vendor or a third-party systems integrator can accelerate the process. Can be time-consuming, with a steep learning curve through the network assessment and RFP/procurement process.	Typically, quicker to purchase as a managed service. Thorough assessment of actual network needs before deployment is still critical, to right-size the solution and avoid over-paying. Managed solution addresses "vendor sprawl" – *i.e.*, managing multiple vendors of various SD-WAN components.
Cost	Ability to shift to cheaper best-effort broadband transport can significantly reduce networking costs.	Expect higher costs but more predictability, esp. in a long-term contract. Service-based consumption model

[27] Some vendors offer hardware-agnostic versions of their SD-WAN products, in which their software can be downloaded as VNFs that can operate on generic "white box" physical servers purchased by the enterprise/agency.

Issue	Do-It-Yourself (DIY) Option	Managed Options
	Can be less expensive overall, but with potential exposure to unanticipated expenses. It is best to compute the total cost of ownership before deciding on a DIY Option.	can be attractive for flexibility and efficiency. In high-growth scenarios, no need to pay for extra capacity until it is actually needed.
Performance	Can be state-of-the art. But may depend on ability to negotiate SLAs with multiple transport providers, finding best deals. Enterprise/agency has full control over what transport options to use.	MSPs are competing on performance, reliability and features. Negotiate an overlay SLA. Some MSPs have incentives to retain customers on their MPLS networks, which may discourage wider use of cheaper transport options such as best-effort broadband and LTE.
Long-term Technology Trends	May need to update installed equipment, at own expense, due to industry consolidation or faster than planned obsolescence. Virtualization and use of "white box" devices will diminish this issue.	Provider bears the risk of keeping up with technological change and industry consolidation. Larger providers may get locked in and be slower to update their bigger installed base.
Security	Some government agencies may wish to retain greater control over their security using a DIY solution. Private enterprise DIYs tend not to fully think through security issues and implement fully-integrated security.	MSP's access to not only packets, but the control data as well, creates security concerns. MSP may have more advanced security tools and experience with using them.

Table 3 below expresses these tradeoffs in the form of a checklist to provide guidance when considering which option best suits your agency's circumstances and telecommunications needs. Of course, a single checklist can't substitute for the kind of detailed, thorough evaluation of all relevant factors (including, but not limited to those described in Table 2 above) that should be undertaken for such an important decision.

Table 3: Checklist for Agency Consideration of DIY vs. Managed SD-WAN

	YES	NO
1. Does your agency have the personnel resources and skills to install and manage a DIY SD-WAN overlay network with minimal vendor support?	☐	☐
2. Does your agency have specialized cybersecurity requirements that cannot be met by a third-party Managed services provider? (Take into account OMB'S updated TIC 3.0 Initiative.)	☐	☐
3. Have you estimated the Total Cost of Ownership for a DIY solution and concluded it is competitive from a cost/value standpoint to a Managed or Co-Managed solution?	☐	☐
4. Have you considered Managed and Co-Managed options and concluded that they don't provide sufficient direct control of the SD-WAN network for your agency's needs?	☐	☐
5. Have you prepared an analysis of your existing WAN's traffic that categorizes it into potential policy-driven profiles matching to the most cost-effective transport options?	☐	☐
6. Do the candidate Managed service providers limit your transport options to only those pre-selected by them?	☐	☐
7. Is your agency willing to negotiate the acquisition and subsequent management of multiple transport options (MPLS, Ethernet, dedicated lines, public Internet, wireless, etc.) to serve as the underlayer network for a DIY SD-WAN?	☐	☐
8. Have you planned out realistic pilot tests and well-defined testing criteria to ensure the DIY solution will apply successfully to your organization?	☐	☐

If your answer to most of those eight questions is a firm "Yes," then your agency might find a DIY implementation of SD-WAN a good fit. However, you should also recognize that there is likely to be a considerably greater investment of agency time and resources for a DIY than a Managed solution, and that the DIY approach may be more difficult to retreat from if the results are not meeting expectations.

5.2 The Co-Management Option

Lying between fully-managed SD-WAN and the DIY approach is the Co-Management option.[28] Reporting on its survey of fifty enterprise IT managers, one market research firm has concluded that co-managed SD-WAN is an attractive strategy for many of them: "[C]o-management comes into its own by taking the operational burden of systems management off the task list for enterprise IT while still allowing them the required control to make changes as they need to."[29] It quotes one senior IT manager who cites control over network security as his primary rationale for choosing a co-management approach:

> We will control SD-WAN policy administration, due to security reasons. We want the policies to be monitored and controlled by us based on our requirements. If we outsource it to third party, then we might end up having polices which are not best suited or secured for our network.[30]

Given these considerations, some Federal agencies may find that a Co-Managed SD-WAN provides the optimum balance, by leaving 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.

The May 2020 EIS Contract Mod for Software Defined Wide Area Network Service ("SDWANS") accommodates vendors' provision of both fully Managed and Co-Managed SD-WAN solutions, so that Federal agencies can negotiate the most appropriate degree of agency vs. vendor control for their particular circumstances.

Three representative use cases for SD-WAN are described below, drawing from MEF's documentation but also known to be successful in actual implementations by enterprises.

5.3 Use Case 1: Managed SD-WAN with Hybrid MPLS and Internet Underlay

One of the most prevalent SD-WAN use cases for private enterprises involves a hybrid network, with both MPLS and Internet-based transport underlays. While MPLS usually provides highly reliable and secure connectivity, its links are relatively costly and it can be time-consuming to add or delete sites to an MPLS network. SD-WAN can establish encrypted paths through either underlay as needed to provide connectivity. Many federal agencies already have an MPLS network in place, making it relatively easy to transition to this type of hybrid configuration.

This use case is illustrated in Figure 3 on the next page.

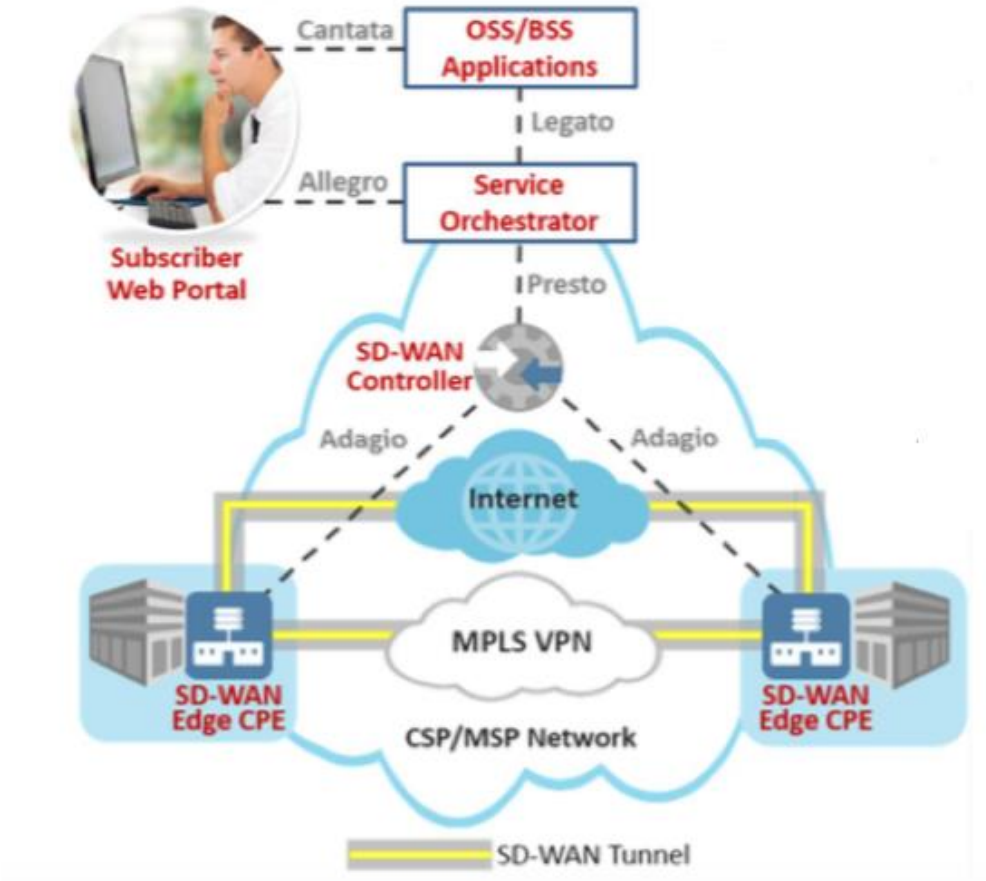
---

[28] Note that for ordering and pricing, however, a Co-Management option is acquired through the same processes as apply for any other Managed SD-WAN.

[29] GlobalData, *Enterprises Are Ready For SD-Wan: They're Just Looking For The Right Partner* (February 2018), at page 5, https://www.centurylink.com/asset/business/enterprise/report/globaldata-sd-wan-voice-of-the-customer-report-cm180646.pdf

[30] *Id.*, p. 5.

Figure 3: Hybrid SD-WAN (MPLS plus Internet) [31]



Adding Internet-based transport (via DIA or best-effort broadband Internet access) and integrating the two via SD-WAN can produce several important benefits:

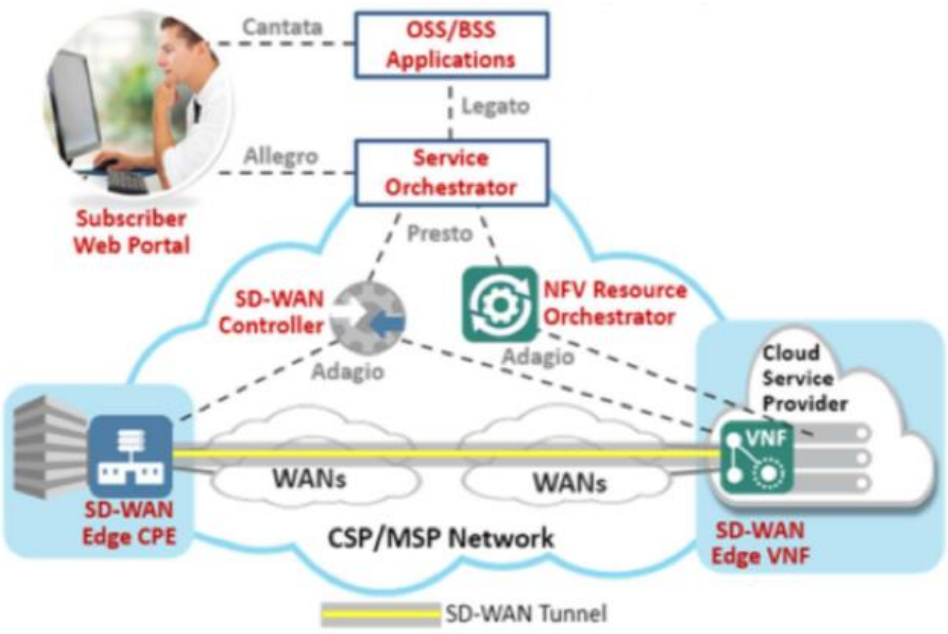
1. When the agency's traffic mix can be segregated into high-priority/high-security level traffic vs. lower-priority/less-secure traffic, then the Internet can offer much cheaper transport for the latter type, conserving MPLS bandwidth for the higher-valued traffic.
2. Under certain circumstances (*e.g.*, when the traffic segregation cited above is less important), overflow traffic from the MPLS can be accommodated by the Internet underlay. SD-WAN can do this routinely to most efficiently utilize available capacity, or it can do this during an MPLS outage (should one occur), to maintain high network availability.
3. As another example of SD-WAN-enabled traffic segregation, SD-WAN can route traffic so that cloud-based applications are accessed directly via Internet connections, at much lower cost than MPLS (which often must backhaul such traffic to a data center).

[31] Source: *Understanding SD-WAN*, p. 10 (Figure 4). (Reproduced with permission of the MEF Forum.)

5.4 Use Case 2: SD-WAN with Secure Connectivity to Cloud Services

Another important use case for Federal agencies is for SD-WAN to provide secure connectivity between agency WAN sites and the cloud applications inside the cloud service provider's data center. As illustrated in Figure 4 below, this can be done by having SD-WAN create paths between the SD-WAN Edge CPE (left side of diagram) and the physical server or virtual machine (VM) where the application is running (right side), in the cloud service provider's environment.

Figure 4: SD-WAN Establishing Secure Cloud Connections[32]



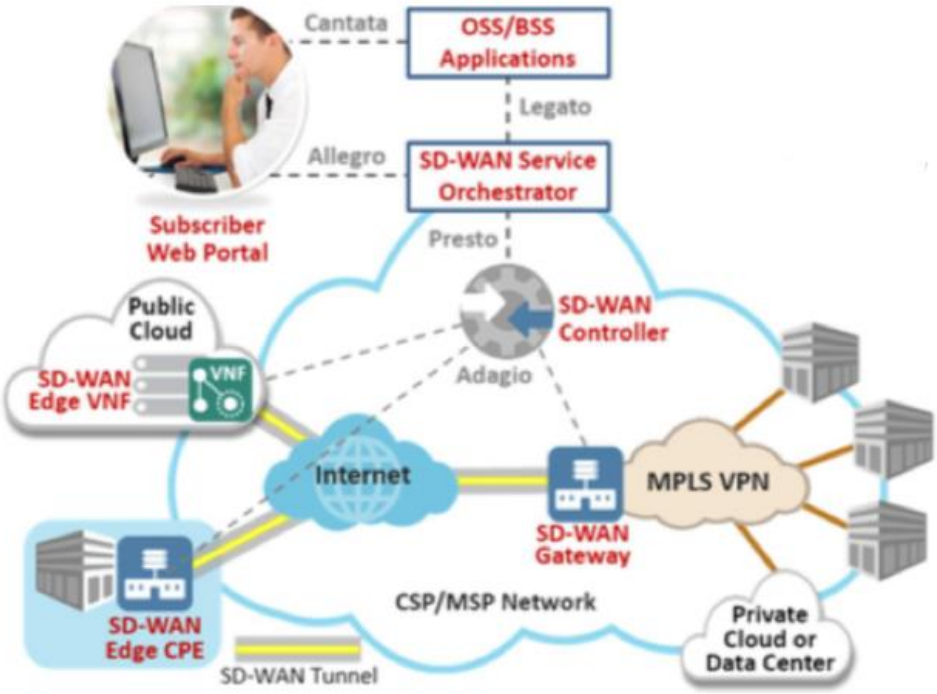
While Figure 4 shows only one cloud-to-SD-WAN connection point, in reality many local cloud connections could be established, essentially at any location where Internet access is available. Given the growing importance and value seen for cloud-based applications in the private sector, it seems inevitable that this will become a compelling use case for many Federal agencies over the next few years.

[32] Source: *Understanding SD-WAN*, p. 11 (Figure 7). (Reproduced with permission of the MEF Forum).

5.5 Use Case 3: SD-WAN to Connect MPLS to Off-Net Sites Using Internet

A third use case of interest to Federal agencies is for SD-WAN to interconnect an existing MPLS network to off-net sites, using the public Internet. This use could be particularly attractive to an agency that has many smaller branch offices, which would be prohibitively expensive to connect to with MPLS alone. In this scenario, a SD-WAN Gateway is interposed between the MPLS network and the Internet. Secure paths can then be established from any SD-WAN Edge across the MPLS underlay to an SD-WAN Edge VNF running in the public cloud environment. This is illustrated in Figure 5 below.

Figure 5: SD-WAN Connecting MPLS to Off-Net Sites Using Internet[33]



This arrangement allows an agency to quickly extend connectivity from an existing MPLS VPN to one or more new, off-net sites using a local Internet connection. This option can be much faster and more cost effective than to build out the MPLS VPN to reach these new sites.

[33] Source: *Understanding SD-WAN*, p. 12 (Figure 8). (Reproduced with permission of the MEF Forum).

6 Key Technical Specifications

SD-WAN is a rapidly-evolving, competitive service, and there is no compulsory standard for the technical specifications of the service. As explained above, however, in July 2019 MEF released its initial voluntary standards for defining the service, *SD-WAN Service Attributes and Services* (MEF 70). The table below summarizes certain key elements of the service as MEF defines it. However, Federal agencies should use the full MEF 70 as their frame of reference for discussions with EIS vendors concerning their specific SD-WAN offerings.

Table 4: SD-WAN Technical Capabilities[34]

SD-WAN Technical Capabilities	
Capability	**Description**
Tunnel Virtual Connection ("TVC") based connectivity via underlay networks	SD-WAN provides a secure, IP-based virtual overlay network (at Layer 3) that typically uses IPsec tunnels through one or more underlay networks, called Underlay Connectivity Services ("UCS").[35]
Operates over one or more Underlay Connectivity Service	Underlay Connectivity Services are the network offerings providing connectivity between the Subscriber sites. UCS can include Ethernet Services (as defined in MEF 6.2 [18]), IP Services (as defined in MEF 61.1 [21]), L1 Connectivity Services (as defined in MEF 63 [22]), and public Internet Services. UCS can use a variety of networking technologies including DSL, HFC, LTE, Wi-Fi and others, and the transport can be based on Ethernet switching, IP Routing, MPLS, etc. UCS performance objectives can be "best-effort" or specified in a SLA.
Policy-Based Packet Forwarding	Agencies can apply policies to make application forwarding (or blocking) decisions for SD-WAN's paths over each WAN. Policies can be based on each application or application grouping, e.g., real-time media or conferencing application. Policy enforcement considers an application's QoS performance requirements or an agency's security or business priority policy requirements. Application Flows can be based on the IP Packet data as well as the Layer 2, 3, and 4 networking headers. Each Application Flow can

[34] Sources: MEF 70 and *Understanding SD-WAN*.

[35] The latest SDWANS mod removed the IPSEC tunnel requirement and now states: "A secure IP-based virtual overlay network over physical IP networks (underlays) using an encrypted connection, compliant with the FIPS 140-2/3 standard for approved cryptographic modules."

SD-WAN Technical Capabilities

Capability	Description
	be subject to a bandwidth (data rate) commitment and limit, via policy.
Internet Breakout	When a UCS is an Internet Service, some Application Flows can be forwarded directly to the Internet, rather than to a TVC. If an Application Flow has a policy for Internet Breakout but Internet isn't available at the SD-WAN Edge where packet ingress occurred, the Service Provider may deliver the packet over a TVC to another SD-WAN Edge for "breakout" to the Internet.
Centralized Management and Control	SD-WAN provides network management, control and orchestration capabilities. These include network monitoring, policy-setting, bandwidth allocation, and other service modifications on-demand. Network administrators and credentialed users can access these functions via a web portal or application programming interface ("API"). In a co-managed implementation, the agency can control aspects of the SD-WAN such as defining Application Flows and creating/modifying Application Flow Policies.
Encryption	SD-WAN Services offer encryption between SD-WAN Edges.
Zero-Touch Provisioning of Site Equipment	Customer premises equipment ("CPE") needed for SD-WAN connectivity can be deployed automatically at a branch office or remote site. Once the CPE is powered and connected to the LAN and WAN, it can retrieve and install its configuration and policies without manual intervention by a service technician at the customer premises.

7 Pricing Basics for SD-WAN

Please visit the EIS Service Guides listing and locate the Basic EIS Pricing Concepts Service Guide to gain an understanding of EIS pricing fundamentals. The pricing structure for SD-WAN varies depending on whether it is obtained as a Managed Service or on a DIY basis. Pricing for these two options are described in turn below.

7.1 Managed Service: SDWANS Pricing Components

The EIS services portfolio now includes Software-Defined Wide Area Network Service ("SDWANS"), which is a Managed Services offering. The price structure for SDWANS is Individual Case Basis (ICB). EIS Contract Section B.2.8.10.1 sets forth the applicable Price Tables and Pricing Instruction Tables for SDWANS. The Pricing Instruction Tables list all defined CLINS for the service.

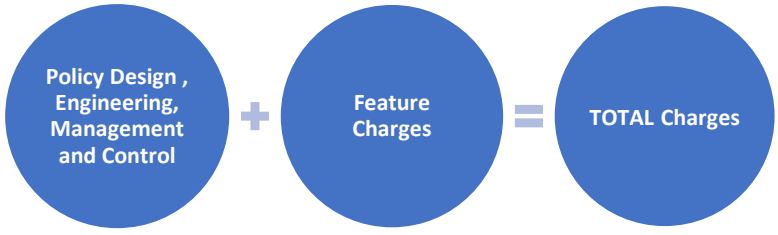
Users of this Guide should refer directly to EIS Contract B.2.8.10 to ensure they have the most up-to-date version of those Tables. The price structure for SDWANS currently consists of the components shown in Table 5 and Figure 6 below.

Table 5: SDWANS Pricing Components

SDWANS Pricing Components	
Component	***Charging Unit***
Basic Charges: Policy, Design, Engineering, Management and Control	ICB
Feature Charges	ICB – for each Feature

Figure 6 below shows how the pricing components in Table 5 are combined to produce the total cost for the service.

Figure 6: How Total Charges for SDWANS are Calculated



7.1.1 Task Order Unique CLINs

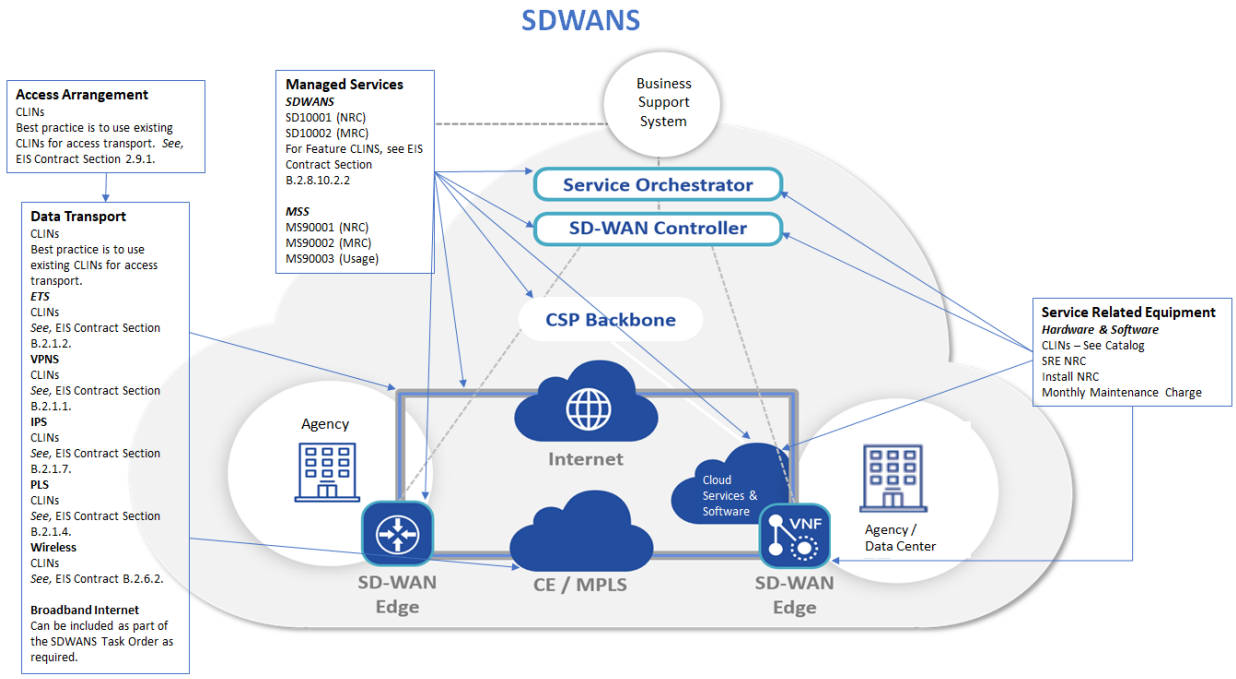
A contractor may offer a custom variation of SDWANS to meet an agency's unique requirements. Such a customization would be identified with a Task Order Unique CLIN (TUC), and would include charges that would have to be added to the components in Figure 6 above to determine the total cost of the service.

7.2 EIS Services Used in Conjunction with SDWANS

Figure 7 below depicts the pricing components of SDWANS. In order to fully implement SDWANS, a user must also purchase certain other EIS services, including Access Arrangements, Data Transport services, and Service Related Equipment ("SRE").

Figure 7: Pricing for the EIS Managed Offering, SDWANS

SD-WAN Service (SDWANS) is an overlay service on top of the Agency data transport networks or underlay.



7.2.1 Access Arrangements

Appropriate access arrangements must be selected for each endpoint, for each Data Transport service to be used in conjunction with SDWANS. See the Access Arrangements Service Guide.

7.2.2 Data Transport

There are a number of different Data Transport service options available in the EIS services portfolio. An EIS Contract Mod is under development for Broadband Internet Service ("BIS"), which is anticipated to be a cost-effective primary transport option for many agencies to use with SDWANs.

7.2.3 Service Related Equipment

- SRE, such as uCPE, must be chosen based on equipment required at each location. NOTE: SRE is priced using Catalog-based Pricing.
- An agency will need to request that the contractor provide pricing for any SRE that would be required, in addition to the agency's existing infrastructure, in order to deliver the service.
- Please see the Service Related Equipment Service Guide for more details.

7.3 DIY SD-WAN: Pricing Components

In order to implement a DIY SD-WAN solution, a Federal agency must assemble it by purchasing the necessary service components and functions from existing EIS services. The following EIS services will apply: Access Arrangements (AA), Data Transport Services, Service Related Equipment, and Service Related Labor. For Data Transport Service, AA is required plus a combination of data transport services (*e.g.*, ETS, PLS, VPNS, IPS, BIS) to connect the various LANs and remote sites on the WAN. SRE is required in order to obtain the SD-WAN hardware /devices and software. Coordination with EIS vendors will be needed in order to ensure that the SD-WAN equipment/devices and software will be made available under SRE. Service Related Labor (SRL) provides the activities necessary to deploy and implement the SD-WAN hardware and software, and is not intended to cover the management-related activities provided by the Managed Services under the Managed SD-WAN service.

This leads to the following pricing components for DIY SD-WAN as shown in Figure 8 and Figure 9 below.

Figure 8: Pricing for DIY SD-WAN

For a DIY implementation, the Federal agency must build up the core SD-WAN network management functions by purchasing appropriate Service Related Equipment from vendor catalogs, together with any needed Service Related Labor.

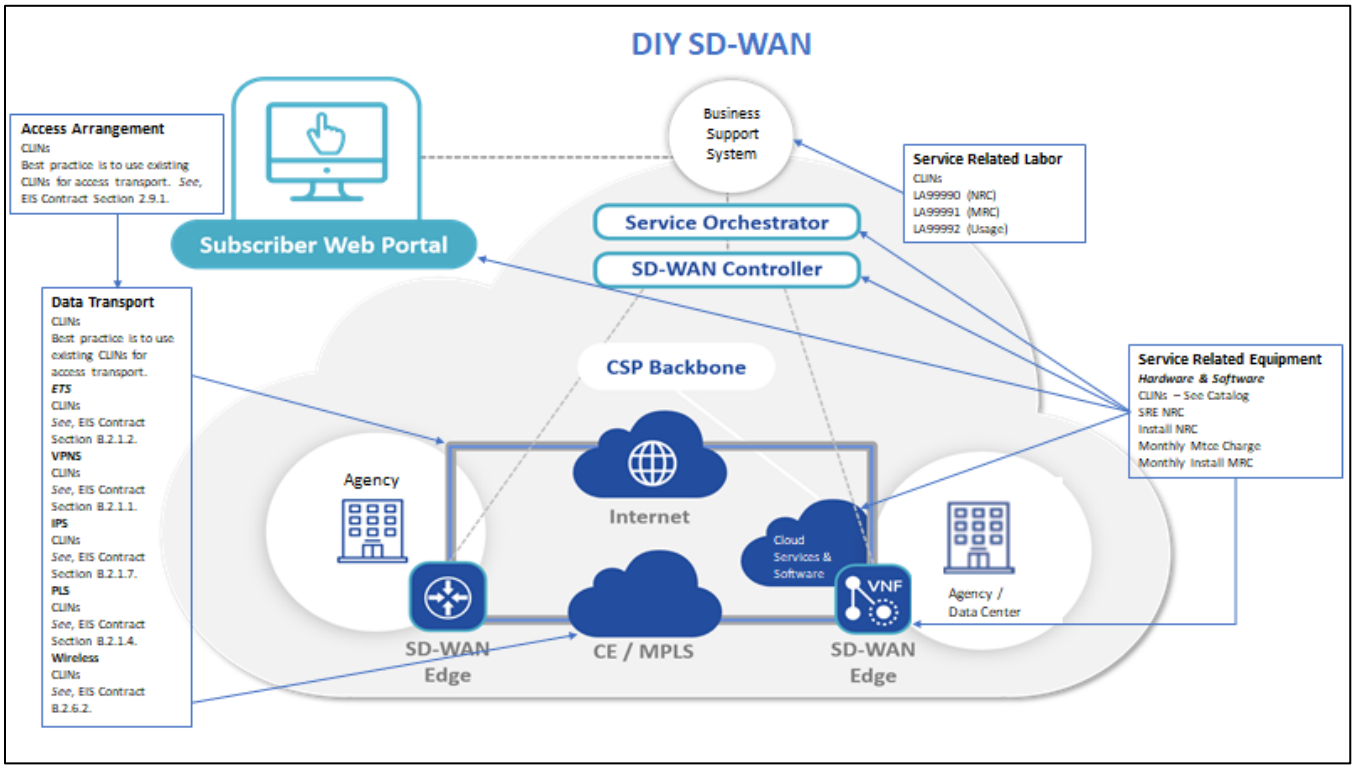
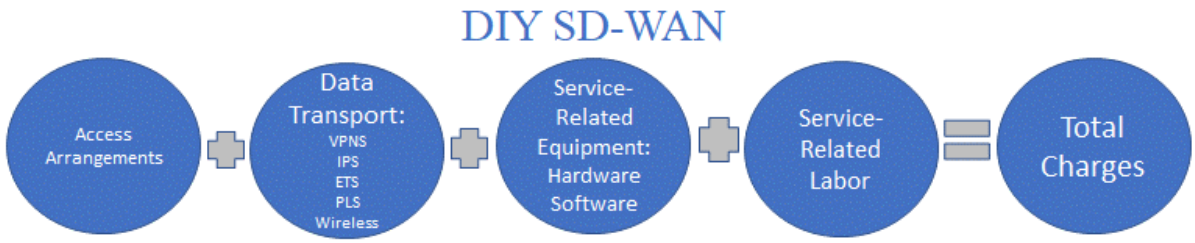


Figure 9: Pricing Components for DIY SD-WAN



7.4 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.

7.4.1 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 access are defined 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.

7.4.2 Data Transport Services

Broadband Internet Access –GSA is working with EIS vendors to develop an EIS Contract Mod for this service offering. It is anticipated to be 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 are 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 are 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 are 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 are 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.

7.4.3 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 shall not be separately priced under SRE. Catalog pricing will be utilized for SRE. 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 shows the pricing elements that shall be provided with each SRE included in a contractor's SRE Catalog. Additional pricing elements may be defined upon request by the contractor.

SRL – labor will be performed on a time and materials basis or fixed price basis. SRL pricing format and instructions tables are found in EIS Contract Sections B.2.11.7.1, B.2.11.7.2, and B.2.11.7.3.

8 References and Other Sources of Information

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)"

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 CLIN list, available at: https://eis-public-pricer.nhc.noblis.org/).

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

Please visit the EIS Contractor's 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).