noblis®

WHITE PAPER

Challenges to Government Adoption of Software Defined Wide Area Networking (SD WAN)

noblis.org

noblis

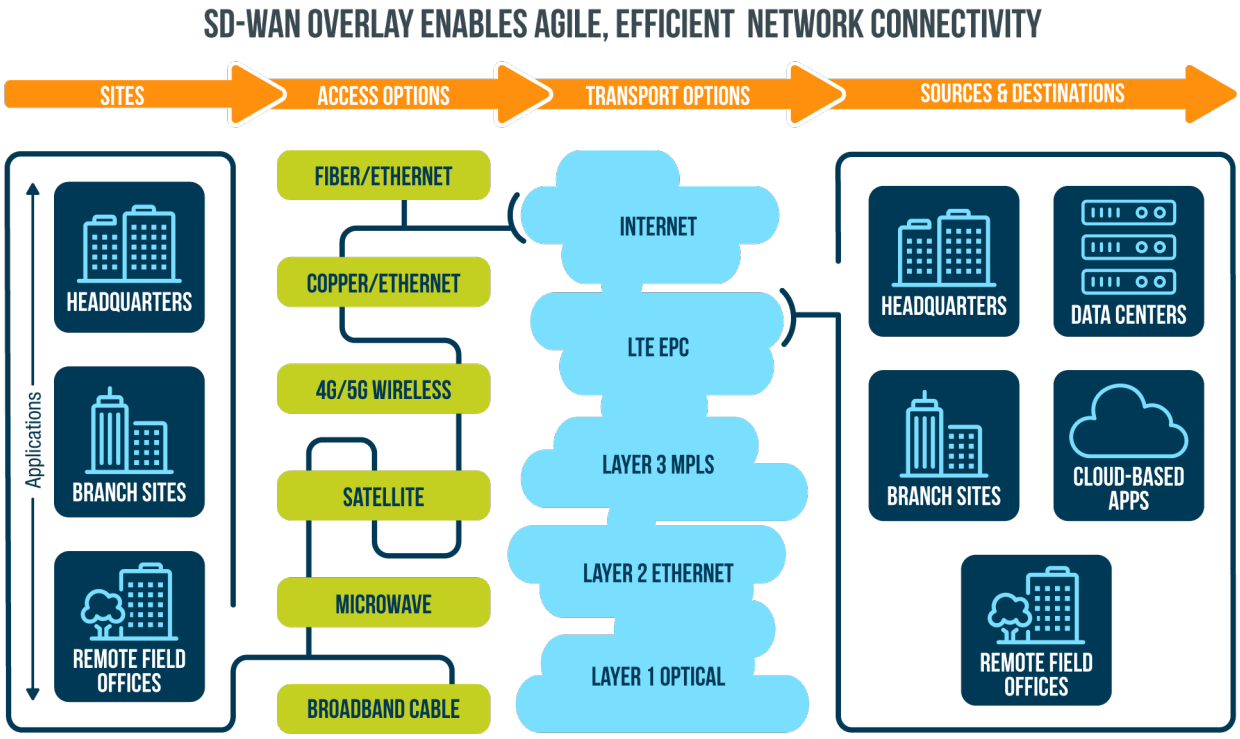
WHITE PAPER

Problem Statement

Software Defined Networking (SDN) and Network Functions Virtualization (NFV) are transformational technologies that will change how the government architects, specifies, acquires, implements, deploys, operates and secures its networks.

Today, telecom providers are deploying SDN/NFV in their commercial networks to lower capital expenditures (CAPEX) and operations expenditures (OPEX), while increasing agility, performance, and resilience. Leveraging those successes, additional services based on SDN/NFV are being developed, rolled out, and vigorously marketed by telecom providers. The most notable of these services is called Software Defined Wide Area Networking (SD-WAN).

Put simply, SD-WAN is a service that combines the agile routing benefits of SDN with the hardware virtualization benefits of NFV at the network edge (i.e., at the customer site). It serves as an "overlay" network that integrates security, policy, and orchestration, using end-to-end encryption between main offices, branch offices, and the cloud. This allows end-user networks to make much more seamless, agile and efficient use of the service provider "underlay" networks (i.e., the physical provider networks that transport end-user communications).



Using SD-WAN, traffic originating at a site can be actively managed based on policies defined by the enterprise. Specifically, SD-WAN allows traffic to be distributed across network connections based on the performance characteristics of the network fabric, matched to the rules (policies) defined by the enterprise.

WHITE PAPER

A particular innovation is the ability to establish different policies for different applications or application groups. For instance, IP voice can be handled differently from critical enterprise data, as could sensitive data vs. non-sensitive data.

In the commercial marketplace, SD-WAN is being touted primarily as a means to avoid the high cost of carrying all traffic over an Internet Protocol - Multi-Protocol Label Switching (IP-MPLS) corporate backbone network. In this business model, high-value or sensitive business traffic is routed across the MPLS backbone, while low-value, less sensitive traffic is shunted off locally to an inexpensive Internet Service Provider (ISP). Application of this business model in government, while appealing, faces challenges due to differences between commercial and government practices, especially in the areas of acquisition and security.

Most agencies are in the midst of transitioning their networking solutions to the new 15-year GSA Enterprise Infrastructure Solutions (EIS) contract, and many are being urged by industry to move to SD-WAN quickly. Before doing so, government telecommunications planners must consider the utility and practicality of SD-WAN in their environments, addressing its potential challenges and adapting commercial SD-WAN technologies and services to their operational and mission needs.

The Practical Scope

SD-WAN is offered commercially both via service providers as a managed service and via product houses for do-it-yourself (DIY) applications. The most important distinction between these two has to do with contracting and operations issues. For example, a fully-outsourced managed SD-WAN service can include the hardware, software, both transport paths and management of the SD-WAN policies that choose between them in a single “buy,” or contracting action. In contrast, a DIY solution can require separate contracting actions to procure the hardware/software and the transport paths, followed by active management/execution of the policies by the buyer. Between these two general categories lies a continuum of alternatives.

Government buyers have a range of providers to purchase SD-WAN solutions from, starting with the vendors of hardware and software products that can be deployed to agency sites. They can also purchase SD-WAN solutions from integrators, telecom carriers and other service providers.

Government telecommunications buyers considering SD-WAN as a solution need to carefully consider the following potential challenges to its adoption:

1. **Technology Transformation Readiness.** Typically, networking technologies currently used by government are static and require multiple single-function devices to be deployed to all but the smallest sites. For example, even a relatively small site may require a router, a switch, a firewall, an intrusion detection system and so on, each housed in a single device and requiring individual, often manual, management and operations functions (installation, configuration, testing, hardware/software upgrades). A fundamental premise of SD-WAN is that multiple devices can be deployed as software applications on a single less expensive physical device, and managed primarily via remote, automated software “pushes.” Furthermore, all but the largest and/or most critical sites in legacy networks are typically connected to the enterprise network by a single physical connection, usually either copper or

optical fiber, while having more than one path for connectivity is a basic assumption of the SD-WAN model.

SD-WAN adoption is not equivalent to moving from older, less capable equipment and connectivity to newer, more capable equipment and connectivity (e.g., from an IP-MPLS network with static routing and T1/T3 access circuits to an IP-MPLS network with more sophisticated routers and Ethernet-over-fiber connectivity). Although difficult, that is still an "upgrade the equipment and circuits" exercise that improves but does not fundamentally alter the architecture of the network. SD-WAN represents a transformational shift in the network's architecture and function. Agencies must understand and accurately assess the consequences of this shift before they will be ready to adopt SD-WAN without assuming significant risk.

2. **Specification and Evaluation.** Acquiring an SD-WAN solution is not straightforward due to the relative immaturity of existing offerings and the multiple ways it can be procured (i.e., as a fully managed service, an agency-managed service, or something in between). SD-WAN is in scope of the new GSA EIS contracts, but is not specifically listed as an available service with pre-defined CLINs. Rather, it can be acquired by taking advantage of the flexibility afforded by EIS, including agency-defined Managed Network Service requirements and available Service Related Equipment (SRE) and Service Related Labor (SRL). Allowing offerors to propose their own specific implementations may result in "apples-to-oranges" proposals that will be difficult to evaluate fairly without significant SD-WAN expertise on the evaluation team. As a result, protest risk could be increased.

3. **Multi-Vendor Networking and Vendor Lock-In.** One of the promises of SDN and NFV, the technologies underlying SD-WAN, is that users can be freed from dependence on a single vendor's solution, also known as "vendor lock-in," and able to implement multi-vendor solutions. While there are open source standards and interfaces in play, the reality is that individual service provider and hardware/software vendor SD-WAN solutions range from largely open with minimal proprietary aspects to mostly proprietary with limited-to-no ability to interwork with another provider/vendor's service or equipment. Agencies must make informed decisions before committing to a specific implementation.

4. **Security.** Federal agencies are subject to the Trusted Internet Connections (TIC) mandate, which requires all outbound and inbound Internet traffic to be screened by the United States Computer Emergency Readiness Team (US-CERT)-developed EINSTEIN system at a secure TIC portal. In current instantiations, this requires all agency Internet traffic to be routed to one of a small number of TIC portals and back. In the commercial marketplace, SD-WAN typically routes traffic to the Internet locally to reduce cost. However, government agencies cannot simply do the same. A new TIC architecture (TIC 3.0) is nearing release by US-CERT, and draft policy guidance from the Office of the Federal Chief Information Officer (https://policy.cio.gov/tic-draft/) indicates a less proscriptive approach that is "friendlier" to modern technologies. However, some uncertainty remains as to how TIC compliance will be achieved for government SD-WAN solutions. Agencies can address this uncertainty by planning a near term technical solution around the TIC Use Cases in the Federal CIO memo and seeking agreement that the solution is compliant. Alternatively, they can limit their use of SD-WAN to alternative architectures that do not use the Internet, such as dual-carrier solutions or

technology/service diversity for network resilience.

5. **Scope and Scale.** Commercial SD-WAN solutions are still relatively young, and not yet widely adopted by major commercial enterprise network owners. One of the reasons is that early SD-WAN offerings in the commercial marketplace did not scale well to serve larger sites. Rather, they were best for small-to-medium locations, at least in part because the hardware employed (typically x86 servers with custom/proprietary enhancements) could not support the necessary scope and scale (number of virtual machines, applications and processing power) needed to serve large sites. While this is improving with every new product development cycle, capabilities still vary across product and service vendors. Agencies must ensure that the product or service offered matches their specific scope and scale needs.

6. **Policy and Governance.** SD-WAN is sufficiently different from legacy networking solutions that existing policies (using the traditional definition) and governance authorities will need to be revisited. In addition, an entirely new definition of "policies" must be accommodated, namely the SDN/SD-WAN definition of policies. For SD-WAN, policies refer to the desired automatic actions that are reflected in software controls to determine routing of traffic at a site based on the data source/destination, application, service, location, congestion level, performance or other characteristics. Typical SD-WAN-related questions that will need answers include:
    - Which operations strategies will be used to determine how traffic is to be routed? What applications or application groups will be included when setting policies? What performance levels will be required by the chosen applications? Are there application-specific SLAs to be incorporated?
    - Will these policies be set and managed at the agency (enterprise) level, or pushed down to the sub-agency or site level? If the latter, what degrees of freedom/authority will be delegated?
    - How will emergency or COOP conditions be handled?
    - If policy guidance changes, how will that be promulgated across the agency?

7. **Operations.** Legacy network operations involve extensive human labor for on-site hardware trouble-shooting, configuration management, hardware/software installation/maintenance/upgrade, etc. This is true even for the managed Virtual Private Networks (VPNs) that are used by the majority of government agencies. A benefit of SD-WAN is that it minimizes (and in some cases eliminates) the need for such labor by replacing physical devices with virtual machines and performing the same functions by software "push." This will require a new "Concept of Operations" (CONOPS) built around less labor, application of more software-oriented skills, and management of policies rather than devices. Among the critical operations questions:
    - Will day-to-day responsibility for managing the implementation and execution of agency-defined, location-specific policies lie with a managed SD-WAN service provider, a separate operations support contractor, or government personnel?
    - What will parallel operations look like, and how will mixed-technology networks operate?

   Agencies must answer such questions and implement the results if their adoption of SD-WAN is to succeed.

8. **Staffing.** With the new CONOPS defined, agencies will need to determine the level of effort and skills mix required from their government and contractor staff. Existing government staff may need to be retrained or supplemented with new hires. Existing support contractor contracts may need to be revisited, recompeted or replaced. Staffing will actually increase as parallel operations begin before eventually falling to new steady-state levels once SD-WAN is fully deployed. Agencies must be prepared for and address such realities.

9. **Contracting.** The new technology and operations characteristics of SD-WAN are not well served by traditional telecommunications contracting methods. These traditional methods typically involve one-time Non-Recurring Charges (NRCs), fixed Monthly Recurring Charges (MRCs), and variable usage charges that can be budgeted for with relative accuracy based on historical traffic patterns. SD-WAN involves contracting for much more dynamic and variable networking, with potential surges in demand, re-routing of traffic across facilities, and perhaps contracts, in real time, and other flexible uses of network infrastructure. Establishing appropriate contracting arrangements and processes will not be a simple cookie-cutter application of traditional contracting approaches. Creative approaches such as pooled usage pricing may be needed.

10. **Budgeting.** Appropriate contracting for SD-WAN must be paired with corresponding development of tailored budgeting arrangements. Budget management at most agencies is highly decentralized, sometimes even when the corresponding contracting arrangements are not. Government budget managers often prefer highly predictable costs with little unexpected variability over time. Costs associated with use of SD-WAN may be more variable than for traditional services, creating greater risk that actual costs may differ significantly from funded budget projections. This is another reason to consider innovative approaches such as pooled usage pricing. Otherwise, maximizing the economies and performance od SD-WAN could result in budgets being exceeded, or, more likely, obligated funds not being spent and lost at the fiscal year boundary. Forecasting costs will be especially difficult in the initial move to SD-WAN, when no historical record is available.

Planning for Effective Adoption of SD-WAN

By thinking holistically and focusing on the real challenges of SD-WAN adoption, government organizations can minimize their risks and achieve a successful and timely adoption. Practical steps that can be taken in the near term include:

- **Obtain expert, non-conflicted analysis and advice** to assess options. Avoid buying into the hype from SD-WAN product vendors and service providers and be cautious about solutions that are not based on open standards. Proprietary solutions will raise the risk of long term vendor lock-in. An expert advisor that is well-versed in government networks and practices but does not have commercial relationships with SD-WAN product or service providers will be better able to inform effective decision-making.
- **Take a holistic approach** to understand all potential benefits and risks, as well as the potential cost impacts (savings and increases) across the enterprise. Consider the technical, performance,

operational, contracting, budgeting, governance and human resources aspects of the transformation. What linkages to organizations and functions outside of the traditional telecommunications domain will need to be established?

- **Establish a roadmap and target architecture** to serve as a starting point for the transformation. While SD-WAN products are mostly sold to service providers, they can be used by agencies wanting to manage their own virtualized, software-controlled networks. Consider the extent to which the solution will use managed services and what functions and responsibilities will be retained in-house. Identify mission-critical applications and support systems needed for a policy- and software-driven network, and plan for a governance structure tailored to policy-driven, application-aware operations.
    - Consider using network APIs to reap the benefits of zero touch provisioning, self-service programmability, and application-aware networking driven by custom software applications.
    - Create a step-by-step roadmap for evolutionary adoption of SD-WAN modernization
- **Include security posture assessment and evaluation** to ensure that the security of your SD-WAN solution fits seamlessly within an integrated enterprise security approach. Assess if you will need more than encryption and stateful firewall services at your sites. SD-WAN can be used to facilitate more efficient use of next generation firewalls and zero trust strategies by moving automated inspection and enforcement points away from the control center, for instance to branch sites or the cloud.
- **Consider prototyping and pilot projects** to gain practical knowledge and reduce risk prior to specifying and acquiring solutions. Vendor demonstrations and pilots can provide sound information. However, tailored, vendor-neutral simulation, stress-testing and analysis will provide greater assurance of effectiveness in your specific environment.
- **Keep future transformation in scope of EIS solicitations** to avoid costly recompetitions. Most Federal entities are preparing solicitations to obtain telecommunications solutions under GSA's EIS program, with Periods of Performance (POPs) of up to 15 years. Focusing exclusively on like-for-like services for the transition to EIS can raise the risk of locking in obsolescence and needing an additional competition to obtain transformational services. If not specifying immediate transformation, include network transformation as a post-transition requirement and include evaluation of a draft network evolution plan in the evaluation criteria. Begin deployment of foundational transformation technologies (e.g., Ethernet) during the initial transition to EIS.

SD-WAN is an emerging solution with tremendous potential for improving the performance, agility, cost-effectiveness, and security of government networks. It represents a fundamental shift in how site communications will be architected, specified, acquired, deployed, managed, operated and secured. It will drive new governance models and forge new linkages between activities across the enterprise. Government organizations that limit themselves to legacy solutions will see rising costs, continued inflexibility, obsolescence challenges, and stagnating performance, while those that adapt will reap the benefits. However, the challenges of implementing SD-WAN can create risks if not carefully addressed.

WHITE PAPER

Noblis offers its government clients deep, comprehensive expertise, non-conflicted analysis and insights, and impartial, hands-on technology assessment services to help navigate the SD-WAN maze to design, acquire and implement a successful solution.

Doing What's Right and What Works for Our Clients

Noblis fosters a culture of collaboration. Through our Centers of Excellence (COEs), we are connecting our staff so that they may better serve our clients. The COEs reach across domain areas and our three companies to ensure the right capabilities, people, tools, and expertise are applied to our work. This enables us to offer every client the best solutions to fit their needs and challenges.

About Noblis

Noblis is a nonprofit science, technology, and strategy organization that brings the best of scientific thought, management, and engineering expertise with a reputation for independence and objectivity. We work with a wide range of government and industry clients in the areas of national security, intelligence, transportation, healthcare, environmental sustainability, and enterprise engineering. Together with our wholly owned subsidiary, Noblis ESI, we solve difficult problems of national significance and support our clients' most critical missions.

Working with Us

Government agencies can access Noblis through a variety of contracting mechanisms. We have several IDIQ contracts in place and available to civilian and DoD agencies. We are also a GSA Schedule holder. For a full list of vehicles, visit noblis.org.

703.610.2000 answers@noblis.org