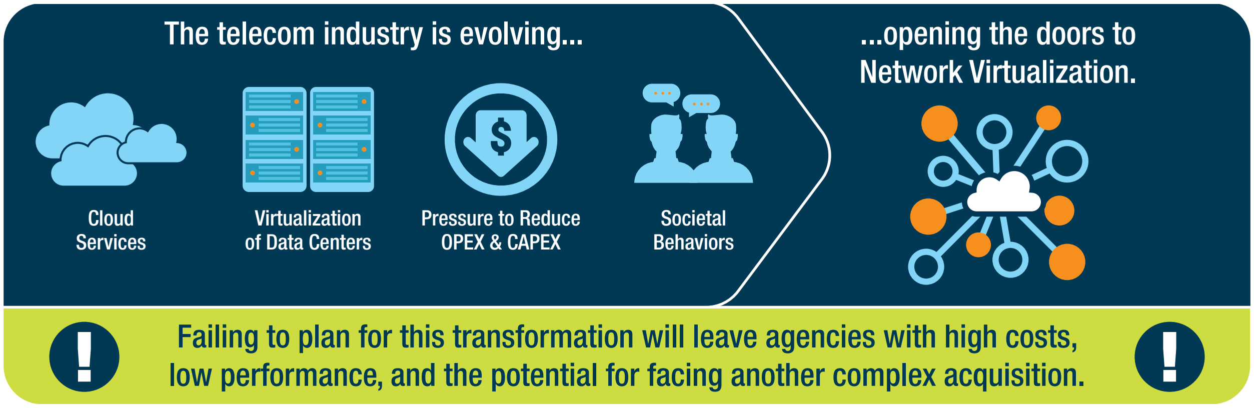
WHITE PAPER

Why SDN Matters to Government

Executive Summary

Network virtualization with software control, reflected in Software Defined Networking (SDN) and Network Functions Virtualization (NFV) technologies, will fundamentally alter the way telecom service provider network infrastructure is architected, specified, acquired, implemented, deployed, operated and secured. Concurrent with this dramatic transformation, most government agencies are planning to transition their networking solutions to the new 15-year GSA Enterprise Infrastructure Solutions (EIS) program. Agencies that understand and incorporate these critical technologies into their planning will capture the considerable benefits while avoiding the associated risks. Those that fail to do so will be left with higher cost, lower performing communications, and likely will face a second complex, time consuming acquisition effort immediately following their transition to EIS. Government users simply cannot afford to be "left behind."



The telecom industry is evolving...

Cloud Services

Virtualization of Data Centers

Pressure to Reduce OPEX & CAPEX

Societal Behaviors

...opening the doors to Network Virtualization.

Failing to plan for this transformation will leave agencies with high costs, low performance, and the potential for facing another complex acquisition.

SDN and NFV technologies matter to government, but each agency must determine how to use them to best serve their mission needs. Agencies should take a holistic approach to understand all potential benefits, risks, and cost impacts across the enterprise, considering the technical, performance, operational, contracting, budgeting, governance and human resources aspects of the transformation. Agencies should seek expert, non-conflicted analysis, advice, and technology assessment such as that provided by Noblis. Doing so can help them to separate marketing hype from reality, understand these technologies and related services in the government context, and chart an effective course to their successful adoption.

In This White Paper

Problem Statement

Network virtualization with software control, reflected in Software Defined Networking (SDN) and Network Functions Virtualization (NFV) technologies, is being deployed into telecom service provider networks to lower capital expenditures (CAPEX) and operations expenditures (OPEX) while increasing agility, performance and resilience. SDN/NFV will fundamentally alter the way service provider network infrastructure (and the government and military enterprise networks that use it) is architected, specified, acquired, implemented, deployed, operated and secured.

SDN/NFV will reduce dependency on complex, expensive hardware, and will require far less human activity for provisioning, software upgrades, maintenance, and service calls to keep government communications flowing. Fewer technicians with specialized vendor-centric skills and certifications will be required to manage and operate enterprise networks, and the need for “truck rolls” should decline significantly. Mean Time To Repair (MTTR) metrics should improve, perhaps dramatically. Use of network resources will become much more agile and efficient, with applications able to interact with the network in real time to get the transport, storage and computing resources they need. Networks will integrate with the cloud more seamlessly and effectively. Network security will become just one element of a holistic enterprise security approach. SDN/NFV will play a critical role in achieving the goals of the Report to the President on Federal IT Modernization, https://itmodernization.cio.gov.

Most agencies are poised to transition their networking solutions to the new 15-year GSA EIS contract. That means planning for the coming technological transformation must begin now.

Government agencies need to better understand these critical technologies in order to capture their benefits while avoiding the associated risks. With most agencies poised to transition their networking solutions to the new 15-year GSA Enterprise Infrastructure Solutions (EIS) contract, the time is now to begin planning for the coming technological transformation. Failing to do so will leave government users with higher cost, lower performing communications, and potentially facing a second complex, time consuming acquisition effort immediately following their transition to EIS.

The Practical Scope

Government and military organizations operate virtual and physical enterprise networks that employ many modern technologies and services, such as IP Multi-Protocol Label Switching (IP-MPLS), Managed Network Services (MNS), Ethernet and Dense Wave Division Multiplexing (DWDN). Many still employ Time Division Multiplexing (TDM) legacy services, especially to provide physical connectivity to their sites. Such solutions remain hardware-centric and operationally inflexible, with high costs, vendor lock-in, long lead times for deployment and upgrades, and security challenges.

Telecommunications service providers are addressing these same issues by aggressively deploying SDN/NFV solutions into their long-haul backbone, regional, and metro access networks. This makes them software controlled, agile, highly efficient and more secure.

> ***SDN allows service providers to replace complex, expensive, vendor-proprietary network routers and other devices with less-expensive programmable devices that can be quickly reconfigured to serve multiple network functions.***

SDN allows service providers to replace complex, expensive, vendor-proprietary network routers and other devices with less-expensive programmable devices that can be quickly reconfigured to serve multiple network functions. Savings come from lower hardware costs, pay-for-what-you-use bandwidth consumption, reduced needs for vendor-certified technicians and network maintenance labor, and reduced needs to dispatch personnel and equipment to solve network problems (“truck rolls”). Network agility and responsiveness are enhanced by the use of programmable controllers that can perform network adjustments and upgrades in seconds-to-minutes that would take minutes-to-months in today’s networks. Network “orchestrators” will provide powerful capabilities to make the network self-aware on an end-to-end basis, regardless of the network elements involved. Orchestrators’ network abstraction allows implementation of policy-driven operations in real time, for both steady-state and anomalous conditions. Security strategies will evolve to take advantage of increased automation and agility.

These benefits do not come without costs, however. Hardware savings will be offset somewhat by higher software costs. Policies will need to be developed to take advantage of the new paradigms. The skill mix of the labor required to operate such a network will change, becoming more software-oriented at the operations level. New security paradigms will need to be developed and implemented.

The implications also go well beyond the traditional network domain, and into data center operations and applications development, where use of SDN/NFV Applications Programming Interfaces (APIs) will facilitate seamless, applications-driven communications across the enterprise infrastructure. Agile software development and Development/Operations (DevOps) practices will need to incorporate the ability to use such APIs appropriately.

As telecommunications service providers ramp up their use of SDN/NFV, the cost of operating networks with older legacy technologies will rise, due to costs being spread across a smaller base of users. Thus government organizations that do not effectively plan for the transformation will not only not gain the associated benefits, but also will see their costs rise as their network performance stagnates. Government users cannot afford to be “left behind.”

Just as moving too slowly to the new paradigms presents risks, so does moving too quickly. Independent Noblis testing has revealed that product claims do not always reflect product capabilities, resulting in the need for careful planning before acquisition and deployment to avoid the potential for serious service disruptions that government organizations cannot tolerate.

For government organizations attempting to plan for the coming transformation, listening to product and service providers is important, but not sufficient. They must separate the reality from the marketing, understand the applicability and limitations of the technology in a government context, and identify a practical strategy for adoption.

Commercial products are developing rapidly and new commercial services are being introduced, but the technologies and marketplace are far from mature. While open industry standards have been developed that promise to facilitate multi-vendor solutions, many of the early market entries reflect proprietary implementations, raising the possibility of future vendor lock-in. Software Defined Wide Area Network (SD-WAN) is an example of an SDN/NFV-based managed service that is being marketed aggressively for its perceived cost/performance benefits. However, the functionality provided varies from provider to provider, and does not always match well with the budgeting, contracting, and security norms of government networks. Most use proprietary or semi-proprietary hardware/software, have limited scalability, have improperly claimed orchestrator functionality, and are not ready to be driven by applications.

In addition, the value proposition of SD-WAN for government may be different than for commercial users. The typical commercial value proposition is moving non-critical data from the "expensive" corporate MPLS enterprise network to "cheap" local Internet access/transport to save cost. However, this is not as compelling for government users who must comply with the Trusted Internet Connections (TIC) mandate, and who may have to execute additional contract competitions to obtain Internet service locally. The value proposition for government may depend more on lower costs to achieve higher availability/performance/resilience by using technology diversity (e.g., MPLS with satellite or 5G wireless for backup), carrier diversity (e.g., dual MPLS providers) or both.

Planning for Effective Transformation

For government organizations attempting to plan for the coming transformation, listening to product and service providers is important but not sufficient. They must separate the reality from the marketing, understand the applicability and limitations of the technology in a government context, and identify a practical strategy for adoption. As the marketplace matures, it is likely that commercial partnerships will be created between product houses, integrators, service providers and management consultants to market solutions, further complicating the effort to make sound, impartial decisions on behalf of government.

! Failing to plan for this transformation will leave agencies with high costs, low performance, and the potential for facing another complex acquisition. **!**

THE NOBLIS NETWORKING AND CLOUD TEST BED CAN HELP.

Test new architectures in conflict-free network and cloud testing center

Access a network management system that Includes network controller and orchestrator

Prepare for future development efforts, especially in the prototyping of mission critical applications

Explore how new networks will enforce strong security policies

By thinking holistically and focusing on the future “to-be” state of virtualized networks with software control, government organizations can minimize their risks and achieve a successful and timely transformation. 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 new entrants, and be cautious about solutions that are not based on open standards. Proprietary solutions may have initial advantages, but they will also raise the risk of vendor lock-in. Likewise, be cautious about nay-sayers who may urge a slow approach simply to extend their legacy revenue streams. An expert advisor that is well-versed in government networks and practices but does not have commercial relationships with SDN/NFV 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 long term plan and target architecture to serve as a starting point for the transformation. While SDN products are mostly sold to service providers, they can be used by agencies wanting to build and manage their own 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 operations.

- 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. 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.

SDN matters for the future of government communications. It represents a fundamental shift in how solutions 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 successfully adapt to these new realities will see improved performance, agility, security and value in their networking solutions. Those that fail to do so will see rising costs, continued inflexibility, obsolescence challenges, and stagnating performance.

Noblis offers its government clients deep, comprehensive expertise, non-conflicted analysis and insights, and impartial, hands-on technology assessment services to help navigate the maze to achieve a successful transformation.

noblis

For the best of reasons

WHITE PAPER

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 subsidiaries, Noblis ESI and Noblis NSP, 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