Using Creative Avenues to Modernize Agency Networks

Providing Government Agencies Access to Telecom Innovation

Federal government departments are at varying stages in their efforts to modernize information technology. Because of the Modernizing Government Technology Act, the President's Management Agenda and Cloud Smart, agencies have no shortage of guidance on what's expected of them. What's less clear, however, is how to acquire the foundational solution – secure high-speed, high-capacity networks – they need to make use of innovative but bandwidth- and data-intensive tools such as artificial intelligence, automation, big data, cloud computing, data mining, and edge computing.

Before agencies can modernize IT, they need to revamp their procurement processes. It used to be that government agencies drove innovation with solicited vendor solutions based on unique problems. Now, agencies are having to pivot to procuring commercially available products, attempting to adjust these existing vendor products and the agency mission requirements to find an acceptable solution. The tradeoff for moving from custom solutions designed for specific missions to commercial products is a reduction in customization and control in exchange for a decrease in time to implement the solutions and lower costs.

"That's an interesting shift within the federal government agencies," said Colin Gosnell, senior engineering leader at Comcast. "But it potentially closes off opportunities to the agencies and vendors alike to bring new innovation to federal agencies."

Longstanding procurement rules such as the Federal Acquisitions Regulation (FAR), which agencies use in their acquisition of supplies and services with appropriated funds, and the Defense Federal Acquisition Regulation Supplement, which sets security requirements for working with the Defense Department, have become so cumbersome that agencies' ability to procure services based on innovation has become overly difficult to administer. It is easier and quicker to procure existing products and contract with vendors with a verified performance history than it is to incorporate new vendors or products into an agency-specific acquisition strategy.

"There is no way to procure new products because there's no vehicle by which to buy them or because the product doesn't focus on a government problem," Gosnell said. The expense new vendors must invest to change an off-the-shelf solution into one that meets federal- and agency-specific acquisition requirements is often viewed as excessive and discourages new, innovative products from being offered to the federal government.

FAR serves a legitimate purpose to protect the government against fraud and to prevent favoritism among vendors, for example, but those requirements are not standard in the commercial world,

putting smaller companies that have not worked in the federal market before at an immediate disadvantage. Government agencies need to understand that, while they are used to operating in highly regulated acquisition and security environments, the commercial entities that they're trying to get these new and innovative ideas from are not.

What's more, one change may lead to others.

An important recent aspect of this challenge to transitioning to newer technologies can be seen in agencies' efforts to move from traditional Time Division Multiplexing (TDM) networking architectures to more modern Multiprotocol Label Switching (MPLS) or Ethernet-based networking. Although commercial customers have transitioned IP, MPLS or Ethernet networking technologies, the federal government has been slow to make similar transitions because of the scope required to transition legacy applications, hardware and infrastructure that was based on a now outdated technology.

Federal agencies must ask themselves, "How do I take my traditional processes running today on TDM and get them across the new Ethernet network? Whose responsibility is it to make sure it operates correctly?" Those two questions alone cause a lot of interagency discussion that introduces delays.

A third obstacle preventing rapid adoption of new technologies is agencies' difficulty in connecting with vendors that have applicable technology. Decision-makers are often mired in the day-to-day operations required to maintain agency missions amid changing economic and regulatory constraints. Successful vendors are able to get in front of agency leaders, prove their concept and identify the procurement path an agency can use.

"Organizations that focus on procurement are a good entrée for companies," Gosnell said. "For instance, the General Services Administration's mission is to bring in more procurement options for agencies, making it an ideal place for a company looking to get government work to start."

GSA's Enterprise Infrastructure Solutions contract is a $50 billion multi-award procurement vehicle that enables smaller companies that aren't traditionally government contractors to compete on a level playing field for government business and encourages large traditional telecommunication providers to provide new, innovative products and services in competition to smaller, nimbler offerors. The contract gives each participating commercial company the ability to offer not only their own service and technology, but also independently offer partner products.

"All those companies that were participants in the award – nine companies – now have an opportunity to seek out any innovative company that can help with the task order that comes out," said Ken Folderauer, Comcast's vice president of federal government sales.

Why the effort is worthwhile

Unreliable networks can sink modernization efforts, resulting in unexpected downtime, degraded interactions with citizens, compromised missions, security breaches, data loss and other unwanted outcomes.

In terms of security, modern options such as Ethernet can deliver to government agencies secure access to cloud and data center resources for seamless connectivity and communications. What's more, Ethernet lets agencies run their cybersecurity requirements independent of the carrier, which could decrease acquisition timelines by simplifying the applicable network security regulations without compromising the agency's security posture. This base-level network segmentation would let agencies implement their own encryption methods, continuity of operations plans and rule sets within their data streams without the commercial carrier being aware of any of it, thereby also increasing security.

Agencies are now looking at ways to buy technology as a whole, rather than using licenses or implementing individual servers in a data center. Several agencies' recent acquisition plans have pointed to a shift from agency-owned network infrastructure to a service-based strategy in an attempt to remove some of the burden of maintaining their IT infrastructure in exchange for increased reliance on commercial services. In these acquisition strategies, increased

security guidelines and acquisition rules have become necessary to control the agencies' exposure to risk when outsourcing IT responsibilities to commercial entities. Unfortunately, these regulations have again limited the available vendor pool and associated innovation.

Cloud computing exemplifies that shift. It elasticizes data, enabling agencies to distribute it and users to access it remotely from a central processing control.

From a technology standpoint, that one element has broken up how agencies are going to consume technology to meet that new base state. From a networking standpoint, no longer are you seeing TDM-based circuits requirements from Building A to Building B. Instead, Building A and B connect directly to a vendor-provided virtual data center and consume associated data independently.

Architecture decisions now center around the origination, storage and distribution of data rather than the physical interfaces between agency facilities. The data and applicable security and regulatory controls can likewise be implemented separately for the underlying network architecture used to transport that data.

Modernization within an agency provides options for network technology to meet the increased capacity demands. One example is Ethernet, a Layer 2 technology that lets agencies separate the control and compliance of the data they send through the carrier from the transport layer itself. MPLS is another widely used network technology that is provided as a managed service and requires some relinquishing of network control to the service provider.

Additionally, agencies have begun using existing internet connections and investigating architectures that allow use of widely available technology over cost-effective internet connectivity scenarios to satisfy data connections to the virtual environment in a compliant, secure manner. The trends should further separation between the data and transport elements in agencies' networking plans.

A Software-Defined Wide-Area Network (SD-WAN), which enables internally controlled secure virtual tunnels built over internet, is giving agencies the ability to manage a single logical network and security control end-to-end while taking advantage of a variety of cost effective access technologies to connected individual physical agency locations.

An agency can use MLPS, Ethernet or internet connectivity-based circuits and layer on an SD-WAN architecture to get a single view and secure control while letting the network act as a single logical infrastructure. We change the conversation from saying, "Give me a total solution for this one problem," to, "Give me a network that can handle my different problems, doesn't tie me to a certain solution set and gives me the capability to adjust my underlying data requirements without having to make large-scale acquisition changes."

Conclusion

Modernization begets modernization. As agencies change their procurement methods, they can more easily acquire the technology, systems and applications they need to meet their missions in innovative ways and disentangle themselves from outmoded, legacy approaches.

Doing this gives agencies greater cybersecurity, increased connectivity, and a solid foundation on which to layer emerging technologies that can make the government more effective and efficient.

Given the stakes, it is critical that agencies understand how to engage vendors that provide foundational IT products and services.