COMCAST
BUSINESS
Powering Possibilities™

4 Steps to Federal Network Modernization

How to achieve a flexible baseline architecture that will support present and future mission goals.

Network modernization can seem like an expensive, arduous process for federal agencies, making it tempting to put off to a later date. While it might feel easier to focus on maintaining processes and tools that are working well enough now, the consequences of neglecting modernization are significant.

Maintaining legacy infrastructure can become expensive and complicated, and can make it more difficult to increase efficiency, help protect sensitive data and achieve broader IT modernization plans. Federal agencies also need the right network infrastructure in place to take advantage of evolving technologies, such as artificial intelligence (AI), machine learning (ML) and edge computing, which require bandwidth, network speed and flexibility.

“Our challenge as an industry in our government-industry partnerships is how to enable agencies to transform through their existing operational models and transition their dated operational models,” says Colin Gosnell, Director of Engineering at Comcast Government Services. “And it’s continuous — when we’re talking modernization today, it’s a different conversation than we had five years ago, or five years before that. It will be continuous and it needs to be all inclusive.”

1. Establish a Baseline

The first step is setting a baseline network architecture that will not only work today, but also positions the agency to meet future needs. The baseline network should be able to handle many different types of traffic and support an array of network characteristics. The goal is to create a network that provides the flexibility to embrace newer technologies over time.

One way to achieve such flexibility is by simplifying the overall architecture, employing a more technology-agnostic, universal approach to modernization. This approach also gives agencies the flexibility to add features to their networks over time. Agencies may not be able to predict the next big tech development, but they should be prepared that, in today's world of fast-evolving technology, the only constant is change.

”Technology trends drive new requirements that we don't yet know the impact of," Gosnell says. "When an agency does a network procurement, they have to do it in such a way that it gives them the flexibility to adjust to those future technology trends integrating into their architecture."

Simplification also applies to a request for proposals (RFPs) and acquisition language. As an example, Gosnell cites an agency procurement for 4G wireless networking services he came across a few years ago.

"The agency needed a way to remotely access data sitting at an on-prem data center. It awarded a multi-year RFP that included MPLS transport to interconnect on-prem data center and offices, 4G wireless for remote access and large internet connects supporting its data center," he says.

Two years later, the agency now favors a cloud topology with a more dispersed workforce that consumes increased bandwidth. The original RFP was so specific to an MPLS, 4G and on-prem-based architecture that the agency will likely have to revamp its entire network to account for updated access technologies. This can result in extended transition timelines and increased costs.

"If the agency had said early on that it wanted to establish a more ubiquitous topology for all of its data, wherever it is located, that would have been a better baseline architecture," Gosnell says. "It would have given them much greater flexibility and wouldn't have required an overhaul. Smaller use-case specific contracts could then be released to different remote access and data-centric services on top of the baseline infrastructure."

2. Choose the Right Connectivity Options

Older agency networks often use legacy technologies, such as Time-Division Multiplexing (TDM), that can present risks and challenges to security and access as time progresses.

"Because agencies were not able to modernize their TDM infrastructure years ago, they are now looking at ways to band-aid their existing TDM infrastructure to keep it operational," Gosnell says. "Meanwhile, network technology has moved so far away from TDM that it's not going to be supported, resulting in a compressed transition timeline and escalating infrastructure availability risks."

As technologies become more dated, the cost — in investment, labor and time — to maintain these technologies increases. Depending on the age of technology, it can be difficult to find replacement parts and engineers who can troubleshoot it.

Federal agencies have some options in moving toward more efficient communications. For instance, agencies can convert TDM signals into Ethernet or IP signals that can travel over an Ethernet solution. While this approach enables agencies to continue delivering TDM service, it's only a temporary solution.

> "We have things like cloud initiatives, edge computing, Big Data, AI, machine learning — there are all these different elements that are out there. To put those all into one modernization package, you're not going to get the best solution for each. You'll get a good solution for all of it, but not the best."
>
> Colin Gosnell, Director of Engineering, Comcast Government Services

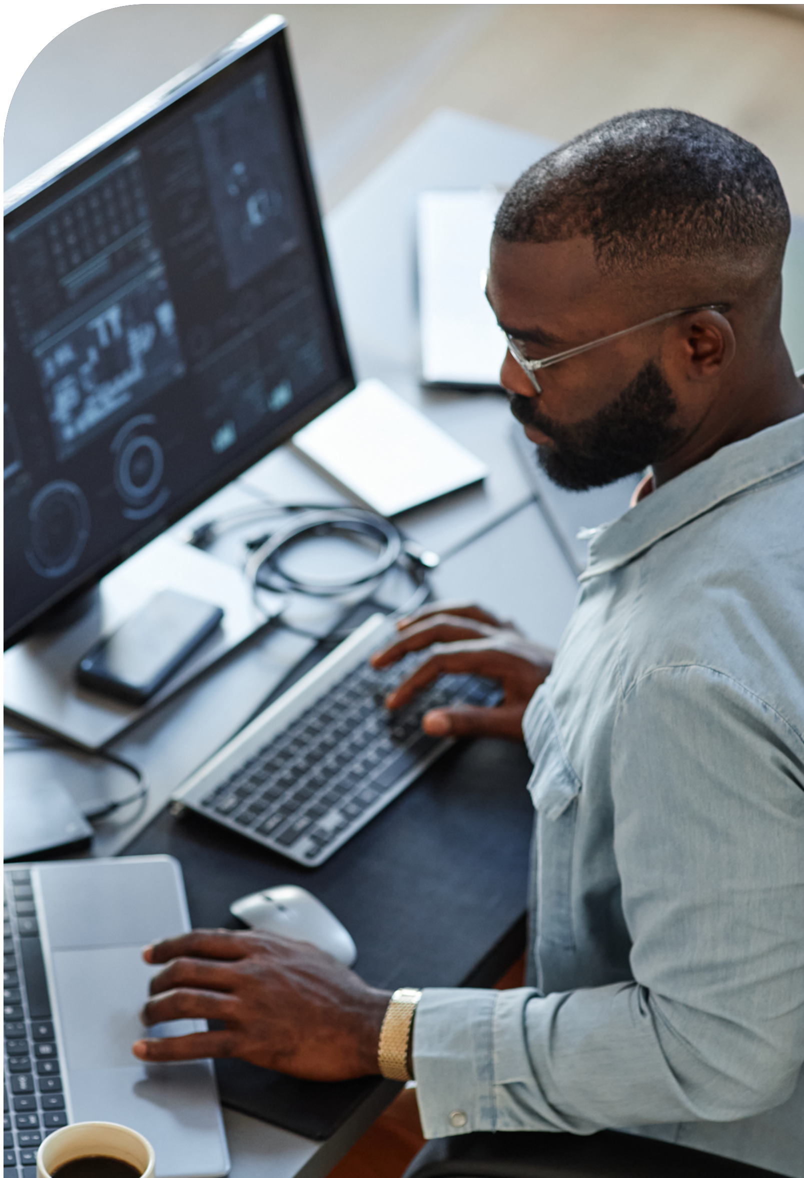
"At some point, there's a crossover where it's no longer working," Gosnell says. "If we don't do the planning on when that crossover is going to hit, which is soon, then agencies are going to be stuck paying those higher maintenance costs for older technology, or potentially just be told they're not going to be supported anymore, resulting in a major mission gap."

For some agencies, the logical replacement for TDM is Ethernet private lines, which provide point-to-point connectivity between locations across a data network. The baseline architecture can handle many different technologies that flow across it. And Ethernet virtual private lines allow agencies to create virtual environments that connect multiple segments with each other. Both types of Ethernet private line technology enable all sites within a specified group to talk to each other and can prevent others from participating. This can help increase network flexibility and security.

Virtual private networks, or VPNs, increased in popularity during the pandemic. VPNs were attractive to agency leadership during the pivot to remote work, because they enabled remote employees to access both cloud and on-premise applications while enforcing agency policies.

When implemented correctly, Ethernet-based private VPNs can provide effective encryption at the data level — from remote devices to servers in agency environments. They also enable agency IT personnel to monitor data traffic flowing in and out of the network. Bridging that gap requires technology that can help provide network security.

Comcast's Business at Home solution establishes a dedicated private Ethernet connection in the remote user's environment and creates an extension from that environment to the agency environment. Agency-specific VPNs can be established, further securing the network data through the entire path while providing the end user a more reliable environment compared to public internet-based VPN architecture. Essentially, this process adds an extra layer of transport security, eliminating the uncontrollable environment of the public internet while still providing required flexibility.



> “Technology trends drive new requirements that we don’t yet know the impact of. When an agency does a network procurement, they have to do it in such a way that it gives them the flexibility to adjust to those future technology trends integrating into their architecture.”
>
> Colin Gosnell, Director of Engineering, Comcast Government Services

Another notable modern network technology is software-defined networking (SDN), a software-based method of controlling the network that relies on virtualized network functions. Federal oversight agencies are bullish on SDN, finding that its flexible architecture is well-suited to large networks and global network infrastructure.

The most important functions for a comprehensive SDN solution include intelligent routing, application visibility, centralized management, policy enforcement, and strong security features like network segmentation.

“SDN is driving edge computing and SASE [secure access service edge] — it’s the baseline for these edge technologies,” Gosnell says. “SDN applications must also be carefully planned so that the use cases are inclusive to the network and the management operations characteristics of the overall architecture.”

Finally, 5G is starting to make its way into Requests for Information (RFIs). 5G has much lower latency than 4G, resulting in faster download and upload speeds — important for edge-computing environments that depend on fast access to data. Of particular interest are 5G private networks.

"Where 5G really is coming into play is in private 5G infrastructure for small locations, where WiFi doesn't necessarily fit the use case of applications. It's an expansion over the WiFi use case," Gosnell says. As an example, he highlighted the impact of a 5G private network on a large warehouse that contains a lot of metal, which disrupts the efficacy of WiFi.

"Private 5G would be able to mitigate that use case and allow for sensors and various technologies to be implemented inside the warehouse," Gosnell says. "So it is very much a topic for agencies, but more of a unique use case rather than a broad technology implementation."

3. Accelerate Transformation

Targeted acquisitions are a key strategy to accelerating modernization. Rather than launching an exhaustive effort to transform every part of the network at once, taking it one step at a time can present less risk and can ultimately produce fast results. By breaking modernization into smaller pieces, agencies can determine which solutions will have the most impact and need to be prioritized.

"We have things like cloud initiatives, edge computing, Big Data, AI, machine learning — there are all these different elements that are out there," Gosnell says. "To put those all into one modernization package, you're not going to get the best solution for each. You'll get a good solution for all of it, but not the best."

In terms of contract vehicles, many agencies are taking advantage of the General Services Administration Enterprise Infrastructure Solutions (EIS) contract, which allows them to pick and choose the technologies they need without having to vet them individually. As new technologies are established, EIS is already in place, making it easier to bring those new technologies on board. SD-WAN technology, for example, wasn't in the original scope of EIS but was added as demand rose. A complicating factor, however, is the speed at which those new technologies are added.

"Agencies' challenge is going to be how to fit the modernization efforts within those products and services defined in the EIS," Gosnell says. "The EIS contract itself is being updated for these new technologies ... but it takes time for EIS to have newer technologies put on it, in order for agencies to acquire them."

Agencies also seek funds available through the Technology Modernization Fund (TMF), which provides loans to agencies for IT modernization projects that demonstrate a strong return on investment. But a comprehensive acquisition strategy needs to employ a balance of contract vehicles and open market acquisitions, Gosnell says.

4. Make Security Non-Negotiable

Federal agencies today know that network security is critical. It's part of every mandate and regulation, from the Federal Zero Trust Strategy to the Executive Order on Improving the Nation's Cybersecurity. Modernization and emerging technologies bring new security vulnerabilities, and when cyber attackers exploit them, costs mount and services can come to a halt.

“Big Data really impacts network security. There are sensors on almost everything that can collect all of this information from what every single laptop in an organization is doing, what servers are doing, what data is flowing through those servers,” Gosnell says. “It’s almost too much.”

With more attack surfaces and angles than ever, the biggest change, he adds, is in the volume of threats. This means that ensuring the safety of an agency’s networks and internet-connected devices is vital. Strategies for modern networks include a focus on zero-trust models, with zero trust network access (ZTNA) for secure application access, as well as SD-WANs and SASEs. These combine cloud-hosted security, ZTNA and advanced networking, enabling remote users to connect securely to resources from any location.

Small businesses that need security features also might consider an add-on solution like Comcast Business SecurityEdge™, which helps Comcast Business Internet customers block threats like malware, ransomware, phishing and botnet attacks across all connected devices. In addition, it helps prevent users from accessing compromised websites and infected links while on the network.

Filtering Out the Noise

Agencies can achieve technology modernization in many different ways, but a consistent challenge for any agency is sifting through seemingly infinite new technologies and developments to determine what is noise and what is most impactful to end users. Procurement strategies can’t be built upon guesswork, but a flexible baseline network will be able to meet the needs of future developments, whatever they may be.

“Procurement strategy deals with what is available today, or what’s in development today,” Gosnell says. “Network strategy helps agency and IT leaders deal with how to support what’s available today and what’s coming tomorrow.”

The challenge of meeting today’s demands while planning for future unknowns is one that is not easily solved. The effort can be worth it as agencies can benefit from an increase in flexibility, reduction in acquisition timelines and increased user support.

❙ Learn more ❙ about how Comcast helps government agencies select and implement the best network solutions to serve their missions — today and in the future.