Mapping the journey to **federal IT transformation**

LUMEN®

Change is now a constant in the federal government IT environment. Contributing factors include new mandates from the White House and OMB, the transformation of federal networks to deliver a digital citizen experience and the need to manage data while securing networks and a growing number of endpoints. Government IT executives are called to deliver an agile, secure environment that adapts with mission needs.

"Agencies need to be able to focus on their missions, not on the technology" said Zain Ahmed, Lumen senior vice president for Public Sector.

Ahmed leads Lumen Public Sector, bringing more than twenty years of experience working with government agencies. No two are exactly the same. Their missions differ and their charters can range from highly focused on domestic issues to international in scope. And those distinctions increasingly affect architectural and organizational decisions as executives look to guide their current IT staffs and environments into the future.

"Every agency is at a different place in the journey," Ahmed said. "We engage them where they are so they can move forward. Listening is one of our key skills."

> **Agencies need to be able to focus on their missions, not on the technology."**
>
> **— Zain Ahmed, Lumen SVP, Public Sector**

LUMEN®

Partners become fellow travelers

Adaptability is key for both the agency and for the partners they work with. In a fast-moving environment with rising expectations – and the mandates designed to drive compliance with those expectations – public and private partnerships are changing. It's about agencies and industry becoming fellow travelers on the journey.

Campbell Palmer, senior director of Public Sector technical solutions at Lumen, outlined three broad categories of engagement that Lumen has invested in to drive effective partnerships.

Categories of industry engagement

Self-service:
The simple things need to be procured as simply as possible. If something is sold as a commodity, such as a bandwidth upgrade for instance, Palmer said that the agency should be able to buy it as a commodity rather than go through a long assessment and quote cycle from the vendor. Lumen developed application programming interfaces (APIs) for many of its products and services so they could be configured by a knowledgeable agency IT person through a customer portal. Human intervention is still an option but for some this DIY approach is quite comfortable and the fastest way to achieve that upgrade. By making the simple things quick, everyone on both sides of the relationship can focus on bigger issues.

Shared responsibility:
Mission-driven planning, execution and management are far more sophisticated than commodities. Lumen platform architects work with agency IT staff to assess long-term needs, develop a program roadmap and design underlying architectures for implementation. Management can be shared, with agency and Lumen teams working seamlessly on their assigned responsibilities.

Managed services:
Streamlining agency IT operations and technology can be accomplished through managed services provided by industry partners like Lumen. This creates flexibility to deploy agency IT staff to other areas of the mission.

Palmer acknowledged that there is plenty of overlap between these categories that make up what he has come to call "the ladder" of engagement. A given program might pull from all three categories of engagement depending on the agency's organizational desired outcomes, underlying architectures, and operational management concerns.

"Agencies like having the ladder," Ahmed said. "They can do it themselves with our tools. Lumen can do it all. Or we can do it together. They can reach as high on that ladder as they need to achieve their mission."

LUMEN®

Staying nimble with a platform approach

Modern, mission-driven challenges are seldom addressed by a single technology or service. It can be misleading when the technology industry mints a new buzzword or acronym such as Secure Access Services Edge, or SASE. It's not a single product or service, even though some might talk about it that way. Many such new developments are frameworks for viewing how a solution might work. Technologies then must be integrated to fill out that framework. And all of those technologies do not necessarily come from the same vendor. Someone just needs to take responsibility for the entire solution.

"By investing in an integrated platform, Lumen can bolster our capabilities with an ecosystem of best-of-breed third parties," Palmer said. "We don't need to be the all-encompassing creator of every piece of a solution. It allows us the freedom to focus on the customer experience. We can listen to what the customer really needs and identify the right solution and integrate it for them."

Incorporating more capability at the edge is a key part of the Lumen platform. Lumen is investing to put data closer to where the customer needs it for improved decision-making capability, low-latency and a high level of security.

The edge also allows ecosystem partners a means of placing their value closer to customers as well. In a rapidly evolving federal government environment, that platform and ecosystem approach can keep agencies nimble as requirements change. And one arena that is constantly changing is the security landscape.

LUMEN®

Seeing the threats before they wreak havoc

Any journey has its hazards. Lumen works with best-of-breed security and technology providers to create a simplified, connected solution.

"There is an intersection of platform and security that is inherent in how we look at the world," Ahmed said. "It's all about the protection of data and the management of data."

In today's new environment, a good partner helps agencies think through their needs and how they can secure the mission without degrading the user experience. The first step is to assume that an agency is already compromised and under attack. This Zero Trust approach, which the Biden Administration has required, encourages agencies to authenticate and verify every user and every device, moving security to the edge. This is especially critical as organizations embrace a hybrid workforce and the traditional network perimeter continues to dissolve. With all these changes, having a holistic approach to security with an expansive view of the network, is critical.

With one of the largest networks in the world, coupled with Black Lotus Labs® intelligence, Lumen scours the network to identify malicious activity and potential threats as they emerge.

This threat intelligence is integrated in a connected security approach to give agencies what they need to be proactive to head off or mitigate attacks.

For instance, the pandemic produced Distributed Denial of Service (DDoS), aimed at taking down websites that shared vaccine information in an effort to disrupt government response. Since Lumen was part of these government agency IT environments, security analysts were able to share insights from Black Lotus Labs and take countermeasures to add resiliency to the government response in a time of crisis.

"One of the good things about owning a large global network is that we can see more of what's going on over the Internet than others," Jason Schulman, Lumen vice president of Civilian Sales said. "Working with our Black Lotus Labs threat intelligence unit, we notice patterns as they develop. We can tell where some attacks are coming from even before the customer notices any impact."

The truth is that someone, somewhere is always probing, trying to find a vulnerability. Security Operations Centers (SOC) are an important part of a proactive, holistic approach to agency security. SOCs are the hubs where security experts command the security technologies, analyze data and manage the agency's security posture. However, top-level security talent is hard to find. It is often cited as one of the biggest gaps in the battle over talent in the economy. Even if you can find top talent, they are just as hard to retain.

The SOC can be offered as a service, often referred to as SOCaaS, which provides visibility across an agency into cyber vulnerabilities and provides fully managed cybersecurity threat detection, incident management support. Building on its existing federal compliant SOCs for customers of Managed Trusted Internet Protocol Service (MTIPS) and Trusted Internet Connections (TIC 3.0), this approach offers more agile response, while alleviating budget concerns. Agencies don't need to worry about finding talent or investing to maintain state-of-the-art technologies in their SOCs. They also cannot replicate the capabilities already present in Black Lotus Labs, the threat research arm of Lumen.

"We run SOCs for multiple agencies," Schulman said. "It takes what could be a huge capital expense for them and turns it into an operating expense they can plan for and budget for. And they get world-class talent and technology."

> **"We can tell where some attacks are coming from even before the customer notices any impact."**
>
> **— Jason Schulman, Lumen VP, Civilian Sales**

LUMEN®

The journey continues

The government IT journey will never end. That's why Ahmed urges agencies to think about adaptability in the network for what lies ahead. There will always be new capabilities to integrate, new demands, new mandates and – unfortunately – new threats to guard against.

That's why it's important to work with fellow travelers.

For more info:

888-597-2455

public.sector@lumen.com

lumen.com/public-sector

LUMEN®