Embrace change and prepare for the future with IT transformation.

Your mission success relies on advanced technologies powered by Verizon.

Learn more at:
verizonenterprise.com/federal-modernization
Federal IT modernization as outlined in the President’s Management Agenda, and detailed in the Report to the President on IT Modernization, calls for a comprehensive approach. The policy integrates long-standing but separate policies for cloud adoption, data center rationalization and optimization, better customer service, improved mission delivery and cybersecurity.

Agency CIO and tech staff must find ways to stitch together these imperatives in ways that serve their longstanding collaboration and data sharing needs – keeping in mind specialized intelligence, national security and cybersecurity considerations.

By acquiring the tools and talent necessary to move all of these strategies, agencies will also gain another benefit. They’ll become more agile in developing and deploying IT capabilities, thereby accelerating the modernizing process.

All of these activities require a focus on networks – those that link agency data centers to one another, those that connect them to cloud services providers, and those that link cloud to cloud. That’s because the hybrid infrastructure model is likely to prove effective as agencies approach IT modernization.

It’s a complicated brew. To bring some perspective to approaching modernization, cyber, and mission delivery, Federal News Network and Verizon convened a panel of federal IT practitioners to discuss these topics.
Examples of modernizing initiatives

Modernization initiatives vary as widely as agencies’ missions. Here are a few of the efforts panelists talked about.

• In some agencies, the need to replace vast stores of paper records persist this far into the 21st century. Shane Barney, the acting chief information security officer at U.S. Citizen and Immigration Services, described “a cave out in Missouri” stuffed with paper records representing 165 million cases. USCIS is converting from paper-driven case handling to an electronic system, called the e-processing initiative. It involves tying together many disparate subsystems using application programming interfaces, rather than building a “grand design” system. The central objective is a person-centered approach with comparable information across multiple subsystems across “billions upon billions upon billions of electronic records.” Barney added, “Networking comes into play. You’re not mailing things, you’re pushing them over the wire. So now we’re building out our infrastructure to support all that moving of data.”

• Chuck Gepford, the deputy CIO at the Government Accountability Office, said, “We’re definitely moving to the cloud” to support his congressional agency’s mission. In so doing, “I think we could be more responsive to our customer base,” Gepford said. “Cybersecurity is foundational to our modernization. Everything from what cloud service provider we’ll choose [to] what kind of connectivity we want in the cloud.” The switch will move GAO, he said, from a capital expenditure business model to an operating expenditures one, with greater financial predictability.

• For Gordon Bitko, the FBI’s CIO, modernization is a state, not a one-time event. “It’s really a cultural change for the organization,” Bitko said. “It’s not typically about any one technology.” He noted, the ever-increasing amounts of crime investigation data FBI agents must deal with has forced the agency’s 56 field offices and its operating units to realize the importance of technology. For the 2013 Boston Marathon bombing investigation, the FBI collected 20 terabytes of mostly video data, Bitko said. “That was an overwhelming amount of data for us at the time. Our network infrastructure couldn’t support it.” The Las Vegas concert shooting four years later resulted in 50 times more data, nearly a petabyte. That “new normal” is driving the FBI to continuously upgrade its infrastructure for handling it, Bitko said. His staff is looking at cloud, its own data centers and applications, and a shared service model for the field offices.

• Commercial nuclear reactor regulation has always been a paper process applied to analog facilities. But Jonathan Feibus, the CISO at the Nuclear Regulatory Commission, said a modernization objective is to get away from paper processes. “So we are pushing to the cloud,” Feibus said. The challenge is updating on-premises-oriented cyber practices to a model that also covers cloud-held data and network traffic to and from remote and mobile users.

Spending considerations

Modernization is primarily about better mission delivery, improved services and stronger cybersecurity. Those might be outlined in the President’s Management Agenda, but they’re also what agencies want to do. Cost and spending are always considerations when deciding how to
proceed. Agencies across the government want to replace legacy code or network infrastructures when the maintenance costs become excessive.

Steve LeFrancois, the federal chief technology officer at Verizon, pointed out that spending patterns on IT and modernization differ between government and industry. He said industry tends to be more comfortable with variable costs based on consumption at a given moment, “and when you reach a certain level of consumption, then it makes sense to put dedicated infrastructure in place.” Whereas government customers prefer more predictable, fixed-rate expenditures.

LeFrancois says that whether a cost reduction or cost avoidance model prevails, agencies need to recognize the real goals of IT modernization. Better mission support, or the ability to meet the mission “op” tempo, requires scalable infrastructure solutions that also deliver continuous evolution. LeFrancois said cybersecurity is also evolving to meet this need. Instead of relying on periodic audits and compliance, “we’re seeing a shift to dynamic analytical models that provide better awareness of what’s being exfiltrated or coming in.” He added, that includes taking “external views of what’s happening” – in effect, pressure-testing networks for the vulnerabilities that might exist.

The NRC’s Feibus offered a case in point. By going to software-as-a-service for email and productivity applications “we were able to avoid having to upgrade all of our servers, upgrade our software licensing.”

At USCIS, Barney said continuous monitoring of cloud spending enables more fine tuning of consumption. In one instance, it found a cloud application no one used between 10 p.m. and 6 a.m. So techs just shut it down for eight hours and watched the cloud-consumption meter drop. That approach lets them rebuild the system daily, resulting in greater security.

For some agencies, shared services offer a way to buy both better cybersecurity and lower costs. At the relatively small Commodity Futures Trading Commission (CFTC), Cybersecurity Operations and Forensics Program Manager Jeremy Christianson said the agency was forced to modernize after the Dodd-Frank law gave it regulatory authority over the swaps markets. Modernizing involves building new applications to analyze market data while protecting the data, and also having sufficient connectivity with the exchanges.

Ultimately, Bitko of the FBI said, “the message that cloud equals cost savings is the wrong message. It’s an opportunity to be more efficient. But we’re never going to spend less on technology tomorrow than we do today. The needs of the organization will be more.” He said a more accurate message to leadership is, “It’s a way of allowing yourself to be more agile and more responsive.” And if done correctly, it’s more secure than legacy infrastructure.

**Technology and cyber considerations**

Modernization for the Cyber Development Directorate at the Defense Information Systems Agency is a comprehensive affair. Acting Director Lisa Belt said it applies to “virtually everything in the defensive cyber operations space, from perimeter to our regional defenses endpoint. And then our big data platform and all our sensors and analytics.” She said the new emphasis is on
“stitching together” the many-point solutions DISA has deployed over the past several years.

Automation of analytics will also be a focus, Belt said. With four million “person entities” in DOD plus tens of millions of non-person entities to be defended “there aren’t enough humans on the planet to throw at our analytics capabilities.” She said artificial intelligence, machine learning, automation, and orchestration will all be elements in an evolving modernization strategy.

Christianson of CFTC underscored the need for automation of IT and cyber processes as a component of modernization. “That’s our motto, for at least this year,” he said. “We need our people to spend time on more important and complex things.”

Verizon’s LeFrancois pointed out how continuous monitoring, cloud, and automation of threat hunting combine to give real-time pictures of cybersecurity and system health – replacing reliance on older FISMA or the Department of Defense Information Assurance Certification and Accreditation Process (DICAP) compliance models with their periodic audits. He said more agencies are adding external scans of their systems as a way of better understanding what’s going on.

Many CIOs and program managers express frustration with their legacy code because it’s hard to find programmers to update and maintain it. And because it’s often not suitable for the cloud. Bitko said the FBI is forced to look at its legacy applications “to figure out what makes sense to modernize. We don’t want to just lift-and-shift legacy applications. That becomes a time-prohibitive and cost-prohibitive direction.” But not always. Barney said USCIS was able to virtualize a 30-year-old COBOL application that processes 70 percent of the agency’s business. The application, its mainframe operating system and its networks were all rendered as a virtual machine running in a cloud. He’s also working with the cloud provider to establish what he called TIC overlays – virtual instances of trusted internet connections. They allow bandwidth to be fine-tuned according to changing needs throughout the day.

Barney also explained how clouds give both agility and cybersecurity at once. A cloud doesn’t require the expenditures of physical security. “You’d never allow a development team to walk in there any time to rack-and-stack servers at will, add more or take out storage, shut things on and off.” Yet that’s normal procedure in the cloud when used as a platform for developing and testing new capabilities.

As the polar opposites of cloud-never to cloud-first give way to a more reasonable cloud-when-appropriate, the notion that cloud computing carries more cybersecurity risk is also giving way. DISA’s Belt called cloud a security enhancement, not a detractor. After all, she said, “the data is roaming the world and you’re looking at a server. That’s interesting, but so what?”

Tom Temin is a Washington, D.C. freelance writer with 40 years in business-to-business journalism. E-mail him at tom@tomtemin.com