March 16, 2017 | The Carr Workplace | Washington DC

Federal Executive Briefing

The Future of Federal Networks

PREFACE

On behalf of the Advanced Technology Academic Research Center (ATARC), I am proud to announce the release of this report documenting the Federal Executive Briefing on The Future of Federal Networks held on March 16, 2017, in Washington, D.C.

I would like to take this opportunity to recognize the following session leads for their contributions:

- **Big Picture Keynote:** John Johnson, Partner at Deep Water Point and Former Assistant Commissioner for Integrated Technology Services, General Services Administration
- **Visionary Keynote:** Chad Sheridan, CIO, Risk Management Agency, U.S. Department of Agriculture
- **Visionary Panel Discussion:** Guy Cavallo, Deputy CIO, U.S. Small Business Administration; Sara Mosley, Acting CTO, Office of Cybersecurity and Communications, U.S. Department of Homeland Security; and Chris Smith, Vice President of Technology, AT&T Public Sector Solutions and former CIO, U.S. Department of Agriculture
- **Collaborative Exchange Facilitators for the discussion on "Bridging The Gap From Legacy To Future Networks":** Dave Mihelcic, Federal Chief Technology & Strategy Officer, Juniper Networks and former CTO, Defense Information Systems Agency; Tim Solms, Vice President of U.S. Federal, Juniper Networks; Chris Smith, Vice President of Technology, AT&T Public Sector Solutions and former CIO, U.S. Department of Agriculture
- **Visionary Keynote:** Dave Mihelcic, Federal Chief Technology & Strategy Officer, Juniper Networks and former CTO, DISA

I also wish to thank the many government attendees who contributed with feedback and their own agency perspectives to our discussion — those contributions certainly enriched the conversation and this report. Among the agencies represented by individual attendees were: Department of Homeland Security, Department of Defense/Defense Information Systems Agency, Millennium Challenge Corporation, Environmental Protection Agency, National Transportation Safety Board, Small Business Administration, Department of State, Department of Labor/Bureau of Labor Statistics, General Services Administration, Department of Interior/Bureau of Land Management, Department of Defense, U.S. Navy, Department of Justice/Bureau of Alcohol, Tobacco, Firearms and Explosives, Government Accountability Office, Department of Treasury/Internal Revenue Service, Department of Agriculture, and the Department of Defense/Defense Technical Information Center.

Thank you to everyone who contributed to the ATARC Federal Executive Briefing on *The Future of Federal Networks*. Without your knowledge and insight, this report would not be possible.

Sincerely,

Tom Suder
President, Advanced Technology Academic Research Center (ATARC)

INTRODUCTION

Federal managers are realizing that, more than ever, their mission success relies upon responsive, capable and well-designed IT infrastructures that can accommodate increasingly heavy data demands, support diverse missions, and service all users securely, regardless of which devices they use.

Trends such as cloud services and big data analytics are already shifting today's commercial and government landscapes. Soon, we can also expect emerging technologies such as the Internet of Things (IoT), fifth-generation mobile networks (5G), and virtual reality to further accelerate data demands on government networks.

Yet while many agencies strive to deploy capabilities to keep pace with these emerging trends, they are often hampered by budget and contracting constraints, an over-reliance on costly legacy equipment, and ever-present security concerns, among other factors.

What options exist as they simultaneously seek to deploy modern capabilities while also serving as effective stewards of limited tax dollars for IT budgets?

In March 2017, the Advanced Technology Academic Research Center (ATARC) — in collaboration with AT&T and Juniper Networks and marketing partners GovLoop and Government Matters — hosted a "Federal Executive Briefing on The Future of Federal Networks." Almost 40 federal executives, IT specialists, analysts and other practitioners discussed how the changing federal landscape is requiring new thinking about how agencies secure and employ network technologies to optimize their evolving IT infrastructures in support of diverse and challenging federal missions. This report is a summary of those discussions and presentations.

To promote a lively and candid discussion, everything said during the event was considered "not for attribution." Consequently, the substantive points and quotations made during the event and included in this report are not attributed to specific persons.

We have organized this report around two themes that dominated the discussion. The first theme concerns the evolving challenges and environments that federal agencies face; the second concerns suggested approaches and best practices to some of those articulated challenges.

CHALLENGES

Terrorism. The economy. Immigration and border security. National and global security. Climate change. Cyberattacks. Public health. The nation's infrastructure. These and other mission-related challenges that federal agencies confront today are diverse and exceedingly complex.

As one speaker remarked: "We are operating in a volatile, uncertain, complex, and ambiguous environment." Effective responses to these challenges necessarily rely on agencies' abilities to effectively harness and exploit information. But today's government networks are incapable of keeping pace with the information demands being placed on agencies.

Federal agency leaders understand that, but transitioning from outdated legacy technologies to modern technologies that offer greater capabilities is complicated by many factors. Among them:

- **Constrained fiscal resources.**

  "There's no money tree. Defense may be getting a boost, but [civilian agencies] are not. The best we can hope for as a civilian agency is that we flatline."

  Continuing resolutions, hiring freezes, budget cuts — these are the new normal. Funding for modernization will necessarily come out of other existing programs and initiatives. Finding funds within the IT budget won't be easy either: Roughly 80 percent or more of IT budgets are consumed by operations and maintenance costs. That means IT leaders must figure out how to simultaneously fix the wing while flying the plane.

- **An over-reliance on legacy technology.**

  "Much of our networking hardware belongs on the scrap heap."

  Critical mission-supporting services run on old technology and code, much of which is beyond end-of-life and constitutes security hazards. Moreover, many employees who know and maintain that legacy equipment are at or near retirement eligibility, which contributes to the organization's risk profile. Finally, these outdated systems consume the vast majority of federal IT budgets today squeezing available funds for technology refresh and needed capital investments.

- **Accelerating demands on government networks.**

  "We're in an era of exponential technology growth … our customers are trying to connect to us and get services in ways that we didn't even know about when we built these networks."

  The dizzying pace of advancing computing power and storage capacity, plus the advent of mobile, big data analytics, and virtualization technologies, have placed incredible data demands upon all commercial and government enterprises. Video, IoT, and, soon, virtual reality and 5G technologies will continue to compound those demands. Most of today's government infrastructures and networks are incapable of answering the resulting data needs of citizens, government employees, first responders, military personnel, and government partners today and tomorrow.

- **Security concerns.**

  "If they're not banging on your network today, they're already inside."

  Effective perimeter security in today's technology environments is no longer feasible. With the advent of an increasingly mobile and cloud-based environment, the perimeter itself — as it has traditionally been defined — no longer exists. So traditional approaches to security — such as strict reliance on firewalls and end-point security — is insufficient. Moreover, the outdated nature of today's government networks and infrastructures — often cobbled together from end-of-life hardware and software — means they are fraught with known security vulnerabilities.

- **An unwieldy acquisition process.**

  "We're in a place where the best technology solution can land in your lap, but you're not able to get your hands on it."

  Poor requirements definition, constraints imposed by contract vehicles or agency policies, lengthy layers of certification and accreditation, and risk-averse behaviors can often stymie an agency's ability to obtain the best available solutions to their business problems.

- **A counterproductive IT buying culture.**

  "I have people that love to buy hardware. … Why is it OK for people to use software to find networking in the cloud, but when you bring it back to the [data center], they want to buy boxes?"

  Employees are often reluctant to buy software-defined solutions. Common practice at agencies involves buying hardware from multiple vendors over time, leading to highly complex architectures that often require having to hire more contractors to integrate it together and maintain it. Technology refresh occurs only sporadically, resulting in outdated hardware and software that cannot keep pace with current demands and that eventually becomes end-of-life, creating security problems.

APPROACHES

While the challenges are daunting, they are certainly not insurmountable.

Some agencies are demonstrating that, despite these hurdles, modernization initiatives can take root and show promise. Doing that, however, requires that agencies adopt new approaches and mindsets to how they think about technology. Among the approaches discussed:

- **Make the business case.**

  "It's not about the technology — it's about the business problems that we solve."

  When budgets are fixed and new technology is needed to move forward, the only feasible approach is to demonstrate the business value of that technology by explaining its importance in terms of the mission. Ultimately, the decision will be made by business leaders, not technology leaders. They need to understand in business terms why a particular modernization path is a higher priority in achieving the mission than other existing endeavors.

- **Think about security differently.**

  "An M&Ms-style security where you've got this hard shell on the outside, but anybody can get to anything on the inside — I think those days are over."

  Security must be layered and baked into the infrastructure. Firewalls and end-point security are important, but the security perimeter must extend to the data itself, wherever it resides. That means data must be encrypted, segmented, and made accessible to select users based on their credentials through smarter software-defined technologies that are easily configurable and automated. More advanced network tools can also provide better visibility into the traffic and behavior on the network so anomalous behavior can be more quickly spotted, inspected, and mitigated when necessary.

- **Bring more creativity and tolerance for smart risk-taking to IT thinking.**

  "What got us here will not survive."

  Agencies should find ways to: simplify their networks and infrastructure; transition away from legacy technology; get out of the business of buying hardware; extend on-premise data centers into the cloud; reconsider current approaches to how staff resources are utilized; and leverage software-defined technology options, such as Network Functions Virtualization (NFV), that are more agile, secure, scalable, and responsive to fluctuating data and bandwidth demands. A way to promote different thinking is to bring in more diversity of thought into the technology planning process. As one participant said: "It's our responsibility to find people from diverse perspectives that can come in and challenge us. The question is how do we value creativity equally with experience?" Another participant added that there needs to be more willingness by agency planners to take smart risks on bolder approaches that take a longer view and have the potential to deliver better performance, security, and mission outcomes. Software-defined networking (SDN) is one such approach and provides a path forward for agencies to replace legacy infrastructure, optimize costs, and improve security. And with NFV, federal agencies have the opportunity to transform their operations from legacy IT equipment into an infrastructure of scalable, low-cost multi-function devices that take advantage of SDN.

- **Procure technology differently.**

  "It's not the core mission of these agencies to buy technology. We need to support the core mission and do it as cheaply and as simply as possible."

  The procurement process must shift more to a consumption-based model. As one participant said: "Our contracting officers view cloud as like buying big iron hardware, as opposed to buying electricity or water. With cloud computing and the network moving forward, we've got to have the same approach. It's got to be, I just turn the tap on and it's there." Another participant suggested that contracts should adopt a credit model for procuring IT capability in which an agency buys credits for a certain amount of capability and then spins up and down its usage as needed until it consumes the purchased amount, however long it may take.

- **Consolidate.**

  "We've got to get past our uniqueness."

  Maintaining many networks within the same department is not sustainable. They are costly, redundant, and increase security risks. Consolidation must occur even when there are diverse missions to support. The answer may not be a single network, but it is certainly fewer networks. For some agencies that still have separate voice and data networks, consolidating those is a good first step, as it often results in increased bandwidth across the network. It is possible to factor in diverse mission needs within a consolidated network, but doing so requires good planning and collaboration, easily configurable solutions, as well as a shared vision of the broader goal. To succeed, collaboration across the enterprise must extend to setting the requirements, the contracting, the concept of operations, and other aspects of implementing the consolidated environment.

- **Get rid of legacy hardware and software.**

  "Blow it up … There isn't a single agency today whose wide-area network and LAN were designed to be what they are today."

  Consolidating networks and infrastructure will help shed legacy applications and systems. So will migrations to the cloud where possible. One manager said he told his staff to figure out the best way to support the mission using today's technology, "and then we'll work out how to get from where we are today to there." One big reason is that outdated end-of-life software and hardware constitute too great a security risk. His advice: "Get current and stay current." He warned that program managers may object that migrating to modern operating systems or other technology will break applications. "My answer is: When a hacker gets into our network, isn't that breaking our applications? I'd rather do it as a controlled break on our side versus an unforced break on their side."

CONCLUSION

Daunting challenges confront federal agencies as they chart their journeys to more modern capabilities that will deliver the needed flexibility, agility, security and performance for current and future workloads. There are powerful imperatives weighing on them to abandon the status quo and get started on that journey. Finding success will require that agencies recognize the need to adopt new mindsets and approaches in how they view technology.

ABOUT ATARC

The Advanced Technology Academic Research Center (ATARC) is a a 501(c)(3) non-profit organization that provides a collaborative forum for Federal government, academia and industry to resolve emerging technology challenges.

ATARC introduces innovative technologies and ideas from academic research labs to the Federal government and private industry.

ATARC holds strategic relationships with FFRDCs such as MITRE, MIT Lincoln Labs and Carnegie Mellon Software Engineering Institute to facilitate emerging technology dialogue between the Federal government, academia and industry.