

WHITE
PAPER

Keeping government modernization on track

with Enterprise IT as a Service.

Introduction

Both the President's Management Agenda¹ and the Modernizing Government Technology (MGT) Act² set goals for government agencies' digital transformation initiatives, emphasizing cost-effective mission performance, service delivery through IT modernization, improved data flow, better workforce management, and expanded partnerships with industry. As part of the effort, agencies in the civilian and defense sectors are increasingly moving to cloud computing to extend their networks and service delivery, while shifting their cybersecurity focus from the network perimeter to the data, devices and users.

Among the hurdles IT leaders face in spurring transformation is the difficulty in determining how to put agency resources to optimal use. Many agencies face an inability to quickly procure services, according to the American Technology Council's recent report on Federal IT Modernization³. Digital transformation efforts to date have often resulted in a mix of systems that can be hard to integrate. But by modernizing and consolidating networks, as well as making use of shared services to enable future networks, federal IT leaders can make strides toward closing gaps in fragmented IT infrastructures.

EITaaS will help unite IT infrastructures and disparate work efforts while at the same time, injecting consolidated IT management, flexibility and scalability into government IT at large.

Faced with increased demand for services, tight budgets, limited staff resources, and mandates to modernize, government agencies are considering what could be the next phase of their information technology (IT) transformation.

Enterprise IT as a Service (EITaaS), which can consolidate IT management in an efficient, scalable environment while freeing up personnel to focus on supporting agencies' missions, definitely fits the bill.

The three elements of Enterprise IT as a Service



Networking



Desktop Services



Compute Storage

How elements of Enterprise IT as a Service come together for government

EITaaS combines three primary areas of IT management that are currently handled separately: networking, desktop services, and compute and store. In those three areas, EITaaS covers high-priority components for agencies, including identity and access management, data protection and disaster recovery and continuity of operations. Bringing these separate elements together under a single “as-a-service” contract, with a commercial service provider, can consolidate the control of operations and modernization efforts. Most importantly, it can deliver key efficiencies for agencies and their IT staff that allows them to shift their focus away from running and maintaining the IT infrastructure to accomplishing their mission.

The Department of Defense (DoD) has taken the first steps⁴ in implementing EITaaS with experiments initiated by the Air Force as well as a plan for a prototype pilot for the Army that’s currently in the works. Both departments are assessing the feasibility of using commercial services for data transport, end-user device provisioning and cloud services. The end goal is to maximize enterprise IT investments while allowing users to tailor services and service levels.

The Air Force called its pursuit of EITaaS a strategic decision⁵ intended to get its personnel out of the business of providing end-user services and refocus instead on offensive and defensive cybersecurity operations, as well as their core mission. Air Force officials see EITaaS as a win-win: The user experience will improve, while they get to focus on their mission, namely warfare superiority.

“The strategic intent is to focus on our core competency,” Air Force Deputy CIO William Marion said in a March 2019 statement.⁶ “Our core competency is to ‘fly, fight, and win’ in air and space. It is not to run email servers or configure desktop devices.”

But the DoD isn't alone in its exploration of EITaaS; federal civilian agencies are also considering the possibilities.

Their approach will be similar: Agencies such as the Food and Drug Administration, the Federal Aviation Administration or the Centers for Disease Control and Prevention can use EITaaS as a way to concentrate resources on their core missions.

Ultimately, a move to EITaaS for civilian agencies could be achieved through several of the General Services Administration's government-wide contracts, such as the \$50 billion Enterprise Infrastructure Solutions (EIS)⁷ contract, recently extended through May 2023, or via Alliant 2⁸, though the GSA may have to offer some guidance for EITaaS. At the moment, the EIS contract is focused on networking, there are eight providers of the contracts, but Lumen is emerging as a leader. Last March, the company became the provider to receive Authority to Operate (ATO)⁹ and the first to receive a task order under the EIS program.

How agencies reap the rewards and benefits of Enterprise IT as a Service

Moving to EITaaS would expand on the benefits agencies get from managed services, as well as further the shift from a Capital Expenditures (CAPEX) environment to an Operating Expenses (OPEX) model. Agencies could then contract for services rather than buying, configuring, operating and conducting end-of-life planning for equipment. A managed service such as EITaaS spares agencies from those costs — in manpower, money, energy and real estate.

The demand for digital information has driven the steady growth of managed services for cloud computing, IT infrastructure and IT security, among others. The managed services market globally is expected to grow 9.3% a year, from more than \$190 billion in 2019 to \$282 billion in 2023, according to a recent report from Markets and Markets.¹⁰ EITaaS in many ways represents the next logical step in an organization's digital transformation efforts, combining areas that have historically been separate.

But the benefits don't end there.

Agencies will realize improved control of their contractors by putting networking, desktop services and storage under one EITaaS umbrella. A typical contract would have a prime, with a number of subcontractors involved for their expertise in specific areas. EITaaS gives agencies greater control from a program perspective with better command of the three vertical areas — network, user services and storage — through Service-Level Agreements (SLAs).

The benefits of EITaaS

- Shift from a Capital Expenditures (CAPEX) to an Operating Expenses (OPEX) environment
- Simplify IT management for network, user services and storage
- Cut agency maintenance costs
- Extended reach and reliability of government networks to deliver real-time applications
- Quick, cost-effective deployment of cloud applications
- Better control of Internet of Things devices

A centralized approach can enable the fast, cost-effective deployment of cloud applications, extend the reach and reliability of government networks to deliver real-time applications, and offer agencies improved control of the Internet of Things devices involved in security, energy use and other functions.

Automation, another pillar of digital transformation, is also enabled by this centralized approach. Automation can be applied in areas across the enterprise, from discovery and provisioning to continuous monitoring and cyber resiliency. In a managed services environment, practically anything can be automated.

The technology is there, it's the execution that is the challenge.

A service delivery model allows an agency to take advantage of new technology developments and innovations as they appear, rather than having to wade through a slow-moving traditional procurement cycle. An EITaaS provider also offers access to experts in specific fields who are familiar with government networks and thus can help agencies optimize their resources. Overall, EITaaS makes IT modernization¹¹ significantly more seamless.

EITaaS offers government a way to propel efforts to modernize IT infrastructure and operations. Instead of a disjointed approach and reliance on outdated contracting methods, agencies can take a holistic, consolidated view from a number of established, flexible contract vehicles. In announcing its plans to test EITaaS, the Army cited the need to move away from established, business-as-usual practices, saying its current pace of modernization cannot meet the service's needs. Just replacing outdated routers, servers and end-point devices worldwide could take at least until 2030.



For government agencies, security is top priority

The bottom line for any government system is security. An agency can't function if it can't protect its data. EITaaS, which consolidates IT and infrastructure and supports the use of standards, can help government agencies reach their cybersecurity goals. Ultimately, the service enables factors that can offer agencies more visibility and control into cybersecurity measures, such as greater agility in software development and greater flexibility in service delivery. Moreover, agencies that turn over IT management to an EITaaS provider can devote their own personnel to the cyber mission, as the Air Force has done within its Air Combat Command.

In addition to the incident reporting and feedback loop that federal agencies have with the Department of Homeland Security's US-CERT, or the military services have with the U.S. Cyber Command, agencies can get another layer of security service from an EITaaS provider. In an era where threats are evolving at a breakneck pace, an EITaaS offering can draw on information around the globe to implement real-time cybersecurity monitoring and practices, fighting threats that typical security teams may not even yet be aware of — and only learn about through a breach.

EITaaS also supports federal civilian and defense efforts to shift the focus of cybersecurity to identity management. Agencies are moving away from securing the network perimeter as the heart of cyber defense to a model that embraces continuous authentication and authorization of users, devices, data and applications, something that can be more easily conducted and managed with EITaaS. This shift addresses the security challenges of operating in a cloud-based, mobile computing world and the resulting threats that target an expanded attack surface. This is why the government has implemented programs such as DHS' Federal Identity, Credential, and Access Management (FCAM)¹² and the Department of Defense's Identity and Access Management (IdAM),¹³ aiming to adopt a zero trust networking model¹⁴ that trusts nothing, verifies everything and enforces the lowest level of user privilege.

Consolidating services under EITaaS also offers the visibility necessary to enforce identity and access management across remote, mobile and Internet of Things devices. An EITaaS provider includes an ID component from the start, which also helps to set the baseline for a Zero Trust strategy.

The managed services market globally is expected to grow by 9.3% a year, from more than \$190 billion in 2019 to \$282 billion in 2023.

Agencies need to carefully transition to Enterprise IT as a Service

EITaaS can simplify IT management for agencies, but getting to that point isn't simple. It's a complex endeavor that requires collaboration with a trusted partner who understands the challenges and has the capabilities to help implement the solution successfully.

Lumen is such a partner. The company suggests that agencies should approach it iteratively, starting with a pilot such as those in the DoD, which involve multiple locations but initially don't involve mission-critical systems. A pilot provides some risk reduction that typically would have an evaluation phase of approximately three years. After that, an agency can assess what's working and what's not before deciding to move forward with a multiyear transition using comprehensive contracting. Both the Air Force and Army recently awarded pilots for their prototype projects.

It's important to note that an agency planning to move to EITaaS should first conduct an asset evaluation to assess what parts of its enterprise could benefit most. Although EITaaS can scale to accommodate any size enterprise, it also can be tailored to fit specific needs or organizations. A large, multi-faceted department such as the Department of Health and Human Services, as an example, could have component agencies that would greatly benefit from EITaaS, even if EITaaS isn't right for other components or the department overall.

The federal government has recognized the need for a fundamental shift in how it procures and manages information technology, with an emphasis on consolidation, innovation, flexibility, agility and partnering with industry to provide services. Enterprise IT as a Service is the path to that.

What to look for in an EITaaS partner



**Broad portfolio
of managed IT
solutions**



**Responsive
account managers**



**Team dedicated
to working
exclusively with
federal agencies**



**Cybersecurity
expertise**



**Competitive and
flexible pricing**

Footnotes

1. President's Management Agenda." <https://www.performance.gov/PMA/PMA.html>
2. "Implementation of the Modernizing Government Technology Act." <https://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf>
3. "Federal IT Modernization." <https://www.cio.gov/2018/05/30/it-modernization/>
4. "Air Force announces Compute and Store agreement." <https://www.af.mil/News/Article-Display/Article/1890934/air-force-announces-compute-and-store-agreement/>
5. "Air Force experiments with commercially provided IT services at eight bases." <https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=12252>
6. "Second experiment for IT services begins at eight bases." <https://www.16af.af.mil/News/Legacy/Article/1778843/second-experiment-for-itservices-begins-at-eight-bases/>
7. "Enterprise Infrastructure Solutions." <https://www.gsa.gov/technology/technology-purchasing-programs/telecommunications-and-network-services/enterprise-infrastructure-solutions>
8. "Alliant 2 Governmentwide Acquisition Contract (GWAC)." <https://www.gsa.gov/technology/technology-purchasing-programs/governmentwideacquisition-contracts/alliant-2-governmentwide-acquisition-contract-gwac>
9. "Lumen is the First Vendor to Receive Authority to Operate Under GSA's EIS Contract."
10. "Managed Services Market by Service Type (Managed Security Services, Managed Network Services, Managed IT Infrastructure and Data Center Services), Vertical, Organization Size, Deployment Type, and Region - Global Forecast to 2023." https://www.marketsandmarkets.com/Market-Reports/managed-servicesmarket-1141.html?gclid=Cj0KCQjwwb3rBRDrARIsALR3XeY4T1mUQhYaVysQW5DoIJ-QMpQ9uEUCY_HWLwVv6dWhe_JGRfYIKrkaAnTtEALw_wcB
11. "Report to the President on Federal IT Modernization." <https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf>
12. "Federal Identity, Credential, and Access Management Architecture." <https://arch.idmanagement.gov/>
13. "IdAM in a Nutshell." <https://public.cyber.mil/idam/idam-in-a-nutshell/>
14. "Zero Trust Cybersecurity Current Trends." <https://www.actiac.org/zero-trust-cybersecurity-current-trends>