Flexera
Inform IT. Transform IT.

WHITE PAPER

Tackling Federal IT Infrastructure Demands

IT Infrastructure Challenges and Solutions in the Context of Zero Trust Architecture

IT Infrastructure Demands as a Government Leader

IT infrastructure costs are constantly sprawling, excessive software and hardware spend can be wasted along with unanticipated vulnerabilities that could cost a fortune. The cost of having no plan to optimize software licensing may face greater pressure when proving IT efficiency.

Federal guidance towards a Zero Trust Architecture means needing to have a clean asset baseline and visibility into your entire IT Asset estate, to identify and mitigate risks before they occur. There are plenty of point products in use that give pieces of this overall puzzle, but we still see manpower as the way that this gets collected, consolidated, and audited.

During a roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Flexera, technology leaders from various Federal government agencies discussed the importance of flexible and optimized IT infrastructure in order to scale operations quickly and to react to changing business conditions securely and efficiently. A strong yet flexible IT infrastructure foundation also allows agencies to strategically plan for future technology advancements and evolving business needs. Roundtable participants discussed the importance of utilizing Zero Trust Network Access (ZTNA) in all current and future systems.

Assessment and Optimization of IT Infrastructure

Panelists agree that having a robust yet flexible IT infrastructure foundation is key to solving and responding to business needs quickly and securely. An early adoption of and migration to the cloud has allowed agencies to react to changing conditions and scale operations to meet urgent business needs. As an example, agencies noted that the mass transition to telework during the pandemic went smoothly due to the strong IT cloud infrastructure already in place.

Several roundtable participants came to government service from the private sector, and noted the difference in culture, strategy, and processes when it comes to government IT infrastructure compared with the private IT environment. While processes may be slower in the government IT environment, a slower process allows leaders to strategically consider all elements of a particular problem to better influence long-term decision-making.

> *Cybersecurity is the most critical business need spanning all agencies, processes, and systems, Roundtable participants agree.*

When considering the steps to assess and optimize existing IT infrastructure, participants shared that they first look for opportunities to save costs and find operational efficiencies. Moving IT infrastructure from legacy systems to the cloud is seen among participants as the foundation required to build all subsequent IT projects, applications, and advancements. To find additional efficiencies, agencies right-sized contracts and reduced the overlap in systems. By narrowing the number of tools to only those needed for core functionality, operational and management costs are reduced.

IT Infrastructure Challenges and Solutions and Zero Trust Architecture

Roundtable participants agree that Federal agencies need an IT infrastructure foundation that is built to accomplish the agencies' mission. The cloud offers incredible flexibility to meet most business needs and serve as a platform for future IT innovation. Early investments in cloud infrastructure gives agencies the ability to quickly scale and pivot critical business operations. For instance, the smooth and secure transition to remote work during the pandemic is attributed to early investment in cloud infrastructure as well as the implementation of Zero Trust Network Access (ZTNA).

Participants are in agreement that the functional nature of IT networks have dramatically changed and will continue to do so. For example, both VPN and MPLS network systems are no longer relevant and should not be a relied upon method of securely accessing networks. Newer technology, like ZTNA, can even be customized with specific security features across a multitude of applications while connected to the cloud. Agencies are working to integrate Zero Trust into all networks and clouds, but are challenged by the manual nature of taking inventory of existing federated systems and to strategically test changes.

The current hybrid remote work environment is causing government IT professionals to analyze the effectiveness of IT infrastructure on critical business needs. For instance, digitizing paper records and quickly sharing mass amounts of data in a secure manner became a critical business need overnight. IT leaders examined ways to facilitate mass digitization as efficiently as possible with a combination of new and existing IT infrastructure. Roundtable participants agree that IT infrastructure will need to accommodate an increase in data sharing as more processes become digitized in the near future.

Future Ready Infrastructure Considerations:

- *Foundation: move from legacy to cloud*
- *Right-sizing contracts*
- *Reduce overlap in systems*
- *Aim for robust, yet flexible*
- *Take lessons from private sector approach to culture and processes*
- *Increase IT training, workforce capacity*

Perhaps the most critical business need spanning all agencies, processes, and systems is cybersecurity. When thousands of government employees transitioned to working remotely in 2020, instead of issuing government owned hardware or relying on dated VPN systems to securely connect to government networks, IT leaders implemented Zero Trust Network Access so employees could use personal computers with an internet connection to access a remote desktop environment without compromising cybersecurity. IT leaders are also examining how Zero Trust Networks can be incorporated with classified networks to better serve the foreign service members working abroad.

Future Ready IT Infrastructure

Roundtable participants discussed several ways IT infrastructure will need to evolve to support new technology and future business needs. IT leaders are already looking at ways to use virtual reality to control building systems and operations remotely and to better connect employees working in the field with higher trained employees who are office based. Leaders are also examining how machine learning can solve business needs more efficiently, such as providing feedback or analytics on live data.

However, in order to implement this new technology, IT infrastructure must be ready with sufficient resources to accommodate advancements. Strategically integrating newer technology is challenging for IT leaders because of the lack of advanced technical experience among existing staff. Leaders are also challenged by the commoditized nature of new, privately development technology that lacks the level of security required of government use.

Panelists also discussed a general lack of IT infrastructure knowledge among generalists in the Federal government, which makes certain business operations more challenging. All agree that training on basic IT infrastructure and the impact of IT infrastructure on government operations should be offered to increase workforce capacity.

When considering the importance and value of IT infrastructure, panelists point to customer experience. IT infrastructure has a direct impact on customer experience, so all decisions should ultimately be made through the lens of the customer.

How Flexera Can Help

Flexera delivers SaaS-based IT management solutions that enable enterprises to accelerate and multiply the return on their technology investments. We help organizations inform their IT with total visibility into their complex hybrid ecosystems, providing the IT insights that fuel better-informed decisions.

Contact us to learn more about Flexera One – a SaaS-based IT management solution designed with and for organizations with highly complex hybrid environments. With Flexera One, you can visualize your entire estate and make data-driven IT decisions from on-premises to SaaS to the cloud.