Maximize modernization in your IT environment

Plan for your real environment, not your desired one.

Today, the world is in the grip of a “digital revolution,” encompassing an explosion of emerging technologies, such as artificial intelligence (AI), robotics, nanotechnology, and more. This provides new opportunities and challenges for safeguarding data in a modernized environment.

There have never been more powerful technology options within reach for the federal government. Many agencies are grappling with how to make the correct choices for IT modernization and cybersecurity, exacerbated by an increased reliance on remote work and a spike in security breaches.

The number of options represent a tantalizing ideal: modernization as an instant, wide-reaching solution to every possible need. This highlights the drive for powerful, cutting-edge technologies and solutions.

Unfortunately, modern platforms don’t always equal secure platforms. Without an acute comprehension of current agency pain points, the realities of legacy systems, and the understanding of agency workflows, modernization efforts can quickly stall and run aground on budgetary, time, and security issues.

For example, agencies may buy or build a new data system, but during the FedRAMP certification process, legacy systems yield unexpected security requirements. At that point, the agency has only one option – spend months and potentially millions of dollars to address and resolve these issues, resulting in a significant delay in efficiency and security.

Agencies do have an alternative with Quest®. Quest is a one-stop-shop for IT decision makers looking to modernize legacy infrastructure and systems. Quest technology provides agencies the ability to fully understand the legacy systems in their environments, as well as solutions to aid in at-scale migrations. This ensures agencies effectively leverage the tools at their disposal.

Quest at a glance

Headquartered in **Aliso Viejo, California**

Established in **1987**

Awarded over **200** patents

> 90 percent of Fortune 500 companies trust Quest

Use cases include business, weapons, classified, medical, SCADA, and cloud systems and infrastructures

It's not about the tools themselves, but how they're used

Challenges with agency modernization efforts often lie in a misconception of what modernization entails. In the face of exciting new technologies and services, agencies may overlook their current pain points as they try to make timely investments in the latest and greatest technology.

Effective modernization is primarily a change in how agencies handle processes within their organizations, including upgrading to modern architectures, containerization, cloud services, and more. However, a robust understanding of the policy and procedures that will govern those new platforms in the next generation of applications and services is equally important.

At its core, modernization is not a one-step effort. Without proper execution and planning, modernization can stall or be counterproductive. Agencies face significant risks due to the complexity of the process and the number of stakeholders involved. IT projects in the public sector are six times as likely to experience cost overruns compared to projects in the private sector. With modernization projects, many of these budgetary issues stem from a failure to set expectations, secure stakeholder buy-in, and address security hygiene.

These budgetary challenges are highlighted by a lack of federal cybersecurity and modernization funding into concrete, planned objectives. Agencies are limited by the requirement to "bucket" costs and benefits within individual accounts, as well as public funds being tied to a particular purpose rather than on-the-ground needs.

Federal cybersecurity and modernization by the numbers

The federal government is expected to spend nearly $19 billion on cybersecurity in fiscal year 2021.

63 percent of federal agencies reported the number of cybersecurity incidents increased in 2020; 65 percent said the severity also increased.

A 2017 Technology CEO Council (TCC) report estimates that the federal government could achieve $110 billion in cost reduction over 10 years by modernizing IT.

Since cyber was added to the FITARA Scorecard in May 2018, the average agency score has risen from D to C.

This system doesn't take into account the legitimate cross-organizational benefits of spending. Individual departments tend to view themselves as distinct entities rather than as part of a larger enterprise, leading to a lack of internal and interagency collaboration.

Overinvestment in modernization with minimal platform or tool comprehension is an equally common pain point for agencies lacking an understanding of internal workflows. Agencies typically have an easier time putting out Request for Proposals (RFPs) for new systems than replacing old ones. Generations of systems across agencies are not designed to adapt to, work with, or build off systems introduced in the previous generation, opening a slew of security issues in the process.

The age of public sector technology and the vast number of obsolete systems, coupled with inconsistent upgrades and patches, represents a huge vulnerability. Modernization efforts are often the resolution to this challenge. But without a thorough understanding of agency infrastructure, platform, services, and applications, as well as how each aspect interconnects, agencies will only inherit their security lapses of the past.

If agencies take advantage of the opportunities the digital revolution has created, and pair these new technologies with improved training, agency comprehension, and a complete modernization plan, they can modernize more quickly and less expensively.

Modernization warrants new techniques and technologies

Modernization challenges don't always stem from outdated, flawed, or inept technology. Instead, they often grow from agencies coping with patched legacy systems, internal silos, bugged software, and archaic cultural ideas. To combat these issues, agencies must first assess where they stand in terms of how they utilize products, staffing, training, and security. The first step for any agency on the path to modernization is to create a plan.

- **Step 1:** Strategic plan with solid goals and objectives
- **Step 2:** Tactical plan with defined budget, timeline, risks, and performance metrics

Both plans rely on improving interagency collaboration and tapping into the right people, including stakeholders and leadership, and ensuring they understand exactly what will change and what is expected of them.

Buy-in from leadership is foundational to the launch of any modernization effort, as transformation requires budget and funding approval. These plans also enable agencies to take actionable steps towards eliminating modernization challenges, such as learning how to staff properly from a security standpoint and the need to improve security hygiene.

In 2019, the United States Government Accountability Office (GAO) completed a review of federal agencies' legacy systems. This report identified the most critical federal legacy systems in need of modernization, evaluated agency plans for modernizing them, and identified examples of legacy system modernization initiatives that agencies considered successful.

Key issues included:

- Continuing use of outdated coding languages
- Allowing unsupported hardware and software
- Operating with known security vulnerabilities
- Lacking complete plans for modernization

These recommendations were provided:

- Reduce the agency threat surface
- Shift legacy code into a modern programming language
- Move legacy software into the cloud
- Identify and document complete modernization plans

Improved security hygiene plays a critical role in making modernization feasible for agencies. Given cybersecurity threats facing the public sector today, agencies need more rapid identification of emerging threats and automated capabilities to detect, analyze, and respond accordingly. Emerging technologies are ready to fill this role, but agencies must proceed with caution.

AI, machine learning, and 5G are not new technologies, but they are newly matured and ready to be leveraged by agencies to lower the risk of new threats. For these technologies to be effective, agencies must implement a series of changes, not in the technologies themselves, but rather in how agencies use and operate their systems. These changes include:

- Strengthen access management, including limiting and understanding who can do what, where, when, and for how long across a network
- Understand that security issues don't disappear through modernization as most lapses are inherited problems
- Implement protections for lateral movement in the event a security breach occurs
- Build a network of trusted partners with a visible, secure supply chain

Agencies often place emphasis on acquiring a product, but that alone will not provide security. The best way to ensure platform and data security within an agency is to fully understand security concepts, as well as how any tool will help with implementation of those concepts.

How Quest can help

The journey to modernization is complex, and agencies need a trusted partner to guide them through potential pitfalls and challenges. Quest offers a variety of software and solutions to manage, modernize, and secure agency enterprise across endpoints, on-premises infrastructure, and in the cloud. More importantly, Quest understands how legacy systems fit into agency environments, and can provide technology-based solutions to modernize those platforms through the following:

- **Data Protection:** Streamlines backup and recovery, recovers unused storage, and develops robust agency continuity strategies across cloud, on-prem, and hybrid environments.
- **Database Management:** Assesses database environment and provides agencies with expert assistance implementing and managing Quest database management solutions.
- **Identity & Access Management:** Redefines agency security posture and tightly secures internal environments.
- **Microsoft Platform Management:** Aids migration, management, and security goals across any Microsoft platform.
- **Performance Monitoring:** Identifies and resolves performance issues with centralized visibility into physical databases and virtual infrastructure.
- **Unified Endpoint Management:** Helps discover, manage, and secure endpoints by accessing agency networks for a more secure environment.

These Quest management methods help to shut down the challenges modernization can present, including patched and unsecured legacy systems, internal silos, bugged software, and archaic cultural ideas. Agencies cannot modernize unless they know what is in their environment and understand the intricacies and dangers of the old system, as well as how they play onto the new, modern platform. Quest serves as a one-stop-shop, capable of managing, modernizing, and securing hybrid environments as well as accelerating disaster recovery across on-prem, cloud, and hybrid. Simultaneously, the technology can fully comprehend legacy systems currently in place and inventory agency networks to maximize the tools already available.

Quest solutions offer completely customizable tools, designed to match customer needs. The company maintains a software portfolio across multiple technologies and disciplines, spanning all layers, from a data center to the underlying infrastructure.

With 63 percent of federal agencies reporting that cyberattacks increased in 2020 and about one-third of federal cybersecurity jobs unfilled, agencies must find ways to modernize that fit the specific needs of their individual organizations.

Proactive investments in modernization solutions lead to a bright future

Modernization can help agencies meet the challenges of the digital age more quickly and less expensively. The federal government sits on the tipping point of technologies, as many innovative solutions and products have matured to the point of being effectively leveraged. Quest offers agencies the ability to utilize these technologies fully, with an emphasis on integration and comprehension of the current legacy systems. The early phases of modernization focused on pushing for the latest and greatest rather than planning for how new technology could best support and work alongside these legacy systems. The future lies in integration.

In 2016, then U.S. Federal CIO Tony Scott estimated that $3 billion worth of federal IT equipment would reach end-of-life status in the next three years. Implementing new technologies and equipment is a cornerstone of IT modernization, but it must be constructed with the foundation – legacy systems – in mind. As emerging technologies continue to develop, integrating now provides a steppingstone to seamless, secure transitions in the future.

To make any modernization effort successful, agencies must look past the tools and towards the policies. Implementing the proper security, governance, people, and policies ensures agencies will be able to learn, train, and prepare correctly for developments later on.

To learn more about IT modernization and cybersecurity and how Quest can help, please visit

www.questpublicsector.com