TD SYNNEX
Public Sector

MAKING GOVERNMENT MORE NIMBLE:

A ROADMAP TO DRIVE INNOVATION IN THE PUBLIC SECTOR

CONTENTS

» **INTRODUCTION**

In government, change can be frustratingly slow.

Point to any city or state on a map, and you'll likely find many of the same challenges: paper-based processes that lead to inefficiencies and less-than-optimal customer service, legacy technologies that lack interoperability, on-premises data centers that increase storage costs, limited data-driven insights that could drive automation — the list goes on.

State and local governments face ever-growing resource and budget constraints. At the same time, citizens expect them to deliver a customer experience that aligns with what the best consumer brands deliver. Technology can help the public sector meet this demand, but IT innovation is easier said than done in government, especially when you consider the public sector's unique challenges: an onerous regulatory environment, limited funding and a workforce with varying skill sets.

State and local governments must build a more agile culture within their organizations and embrace technology disruption to meet the 21st-century needs of their constituents.

But what exactly does an agile government look like?

The National Association of State Chief Information Officers (NASCIO) surveyed IT leaders from all 50 states to assess their top policy and technology priorities for this year. NASCIO's State CIO Top 10 Priorities for 2020 indicate that while many technology and policy goals have remained consistent for IT leaders in recent years, emerging technology and changing attitudes about how government should best serve citizens are reshaping their IT agendas.

Public sector CIOs need to develop a modern, agile IT infrastructure within their organizations. The 2020 survey shows that CIOs are keenly focused on addressing years of technical debt and embracing more innovative and flexible technology approaches. Six out of the top 10 priorities identified in NASCIO's survey map directly to these crucial business priorities:

1 / Building a foundation for digital government
2 / Innovation and transformation through technology

3 / Moving toward consolidation and optimization
4 / Embracing cloud technologies and services
5 / Improving cybersecurity and risk management
6 / Better data management and analytics

Creating a modern foundation for digital government will require government IT organizations to adopt a DevSecOps approach, which involves automating their technology infrastructures and workflows to improve collaboration between developer and operations teams and to accelerate the development-to-production life cycle. With enterprise open source technologies, state and local government CIOs can begin to cultivate a DevSecOps culture within their IT organizations. They also can leverage this technology to optimize their resources and create more flexible systems. Here's how state and local governments can use this approach and open source principles and practices to build a foundation for digital government, integrate innovative technologies such as the cloud and data analytics, and achieve their ultimate goal: delivering a better citizen experience. **»**

NASCIO's State CIO Top 10 Priorities 2020

1. Cybersecurity and Risk Management

2. Digital Government

3. Cloud Services

4. Consolidation/ Optimization

5. Customer Relationship Management

6. Budget, Cost Control, Fiscal Management

7. Legacy modernization

8. Data Management and Analytics

9. Broadband/Wireless Connectivity

10. Innovation and Transformation through Technology

A FOUNDATION FOR DIGITAL GOVERNMENT

Digital government has been the driving factor for technology modernization in the public sector over the last decade.

At its core, digital government is about using innovative technologies to transform how government does business, driving more value for constituents in the process. Each of the five other NASCIO priorities we've outlined — driving innovation and transformation through technology, adopting cloud solutions and services, undertaking consolidation and optimization projects, better data management and analytics, and robust cybersecurity and risk management — are foundational elements for enabling digital government.

"When you look at digital government, you have to get to the root of why technology matters for government more so now than ever before," says Frank DiMuzio, Regional Manager, Emerging Technology at Red Hat, a leading provider of open source solutions for the public sector. "Government is under pressure to provide an experience to citizens through technology that is similar to what consumers experience in the private sector, but they have a lot of constraints, whether it's regulations, security, confidentiality of information or even just how their information is stored."

For the public sector to make digital government a reality, government organizations must address their technical debt, create processes and systems that improve inter-agency sharing and leverage open data — at least among their peer agencies within a given state, says DiMuzio, who works with state and local government agencies across the country.

"The Department of Health and Human Services should be able to talk to the Department of Taxation, and they should be able to talk to the Department of Motor Vehicles as part of that citizen experience," he says. "The last thing someone wants to do is enter the same information they've already entered into a state, county or city web page."

Using insights and feedback from constituents, along with strategic inputs from key stakeholders and business needs assessments, can help organizations map out a modernization strategy that enhances the citizen experience. Strengthening their IT infrastructures will be core to this strategy.

Some of the key capabilities and technologies governments need to become more agile include an open source-based standard operating system that can accommodate hybrid cloud environments; cloud-based solutions that reduce storage costs while accelerating innovation; a container platform that streamlines application development, production and deployment; data analytics that improve decision-making; and privacy-focused technologies with built-in security that improve state and local governments'

Becoming More Nimble

To become more nimble, governments need the following capabilities and technologies:

- **An open source-based standard operating system that can accommodate hybrid cloud environments**
- **Cloud-based solutions that reduce storage costs while accelerating innovation**
- **A container platform that streamlines application development, production and deployment**
- **Data analytics that improve decision-making**
- **Privacy-focused technologies with built-in security**

cybersecurity posture, reduces their risks and protects citizen data.

All these things can help agencies focus on three of the most critical requirements for digital government: embracing modern technologies, automating processes and services, and embarking on cultural transformation to break down silos between IT and non-technical teams.

However, digital transformation is an ongoing journey. It often must happen in stages. While digital government is the end goal, the public sector must be methodical with how it reaches this destination and focus on both short-term and long-term strategic goals. State and local governments can start this journey by driving innovation and transformation through technology. **»**

DRIVING INNOVATION & TRANSFORMATION

To drive innovation and transformation, state and local governments must find new ways to develop and deploy technologies.

However, innovation and transformation can't just be relegated to the technology itself. It has to happen hand-in-hand with cultural change within government IT organizations. Embracing a DevSecOps approach — driven by open source principles and practices — can help state and local governments achieve cultural and digital transformation.

A DevSecOps approach involves creating an adaptive and collaborative culture. However, this is especially difficult for government IT teams that have traditionally operated in silos and have often lacked "a shared set of tools they can use across the organization to knock down technological barriers to speed time to production," DiMuzio says.

Changing your organization's culture may seem like a constantly moving target, but the open source community provides a blueprint for the types of principles, processes and technologies public sector CIOs can adopt to drive innovation.

"Open source has proven to be that engine of innovation. If you look at some of the most notable brands and names today, none of these companies would have been able to scale and meet the demands of users had it not been for the innovation that open source has provided. At the highest level, that's how open source technology and processes can help the public sector," DiMuzio says.

Government agencies must discover a new way of working, and to a certain extent, embrace a startup mindset. The open source community provides a roadmap for how to accomplish this. Red Hat Open Innovation Labs, for example, uses processes and best practices from the open source community to create a culture of collaboration and advance innovation within organizations.

In Open Innovation Labs, Red Hat consultants and experts collaborate with cross-functional teams, giving them the tools, knowledge and framework to come together to tackle a key business challenge within their organizations. The approach involves building trust and transparency within teams by engaging in exercises such as impact mapping, a strategic planning technique that enables teams to ensure the products they are working on align with their organization's goals; embracing rapid development and experimentation and a "fail

> **"If you look at some of the most notable brands and names today, none of these companies would have been able to scale and meet the demands of users had it not been for the innovation that open source has provided. At the highest level, that's how open source technology and processes can help the public sector."**
>
> – Frank DiMuzio, Regional Manager, Emerging Technology, Red Hat

fast" approach; and creating a feedback-centric environment to capture new ideas and learnings. Using this method, teams can bring diverse skill sets together and create new software or modernize existing applications their organizations can scale to accelerate their digital transformation.

UNICEF Innovation, which is focused on using technology to address global humanitarian issues that affect children, has benefited from this approach. The organization has worked with Red Hat experts to enhance a School Mapping Project tool. The tool is designed to make it easier to gather real-time data from universities, data scientists and research institutions, allowing UNICEF to build more robust evidence that will drive humanitarian initiatives to increase access to education and information in developing countries. The

tool also will help UNICEF "make decisions more quickly, streamline the integration of new data, and improve emergency response and resilience against natural disasters and crises."

Some agencies may not adopt this specific type of engagement to make themselves more responsive. However, they still can draw on best practices from the open source community to begin driving a culture of innovation, communication and collaboration, especially when it comes to breaking down organizational silos. As collaboration becomes the norm rather than the exception for government agencies, they can begin to work across traditional boundaries to reduce technical debt and to adopt open source solutions and other emerging technologies that help them build a solid digital foundation. »

MOVING TOWARD CONSOLIDATION **&** OPTIMIZATION

Consolidation and optimization — which involves combining services, operations, resources, infrastructure and data centers and embracing enterprise thinking within organizations — remains a high priority for CIOs because it is foundational to government transformation initiatives.

NASCIO data indicates that as of 2017, 46 percent of states had completed consolidation initiatives, while these efforts were ongoing in 42 percent of states. One of the largest states in the U.S., for example, has consolidated 50 departmental IT organizations and is gradually moving toward consolidating all agencies into one state-of-the-art data center. The move has allowed the state to adopt an enterprise-wide approach to security, budget management and governance while also consolidating applications to streamline citizen service.

Admittedly, efforts like this can be costly and time- and labor-intensive. However, they also produce long-term cost savings and efficiencies for state and local governments, while giving them the capacity to enhance data security and integrate modern technologies like the cloud. Still, the public sector's consolidation efforts won't be as impactful if government agencies don't standardize their IT infrastructures — and this has to begin with legacy modernization.

"The modern, digitally capable government agency is one that is agile and responsive to citizen requirements, and there's no way to do that without having an automation capability. For them to do all these really incredible things in the cloud and develop cloud-native applications, they really need to have this capability," DiMuzio says. "The only way you can really automate is by standardizing. You can't automate environments that are very heterogeneous."

Standardization benefits government agencies in several ways by enabling them to:

- **Reducing IT complexity** allows agencies to reduce IT workloads, storage and maintenance costs.

- **Adopt modern solutions:** Agencies can move more quickly to the cloud and begin to use interoperable solutions that enable automation and predictive analytics capabilities.

- **Make solutions configurable:** Agencies can become more flexible and agile and avoid a high level of customization that leads to vendor lock-in and technologies that quickly become obsolete or can't meet evolving business requirements.

■ **Realize additional cost savings:** With less IT complexity and access to modern solutions and data-driven insights that improve forecasting and budget planning, agencies may have more money to invest in improved service delivery and new citizen services.

A modern, standard operating environment should be capable of handling enterprise workloads, providing a solid IT foundation for agencies to address critical business tasks — whether that's eligibility determinations for health and human services programs, better workforce management for public safety departments or facilities management for parks and recreation departments.

It also should have built-in security controls that enable state and local governments to automate upgrades, regulatory compliance and security management, and provide a portable, scalable infrastructure that can accommodate hybrid IT environments. A modern, standard operating environment also must provide insight capabilities that continuously monitor and proactively repair security, performance and reliability-related issues before they cause service disruptions. Eighty-eight percent of public sector agencies have experienced at least one cyber attack in the last two years, so as government agencies

face more security vulnerabilities, this capability is especially critical.

Bill Hirsch, principal solutions architect at Red Hat, says state and local governments can't afford to bypass standardization as they proceed with modernization initiatives.

"The most important thing is adopting a standard operating environment, because without standards, government agencies are going to be constantly spending more time on easily automatable tasks at the expense of time for innovation," Hirsch says. **»**

Where do states stand on consolidation initiatives?

42% of states have ongoing consolidation initiatives.

46% of states have completed consolidation initiatives.
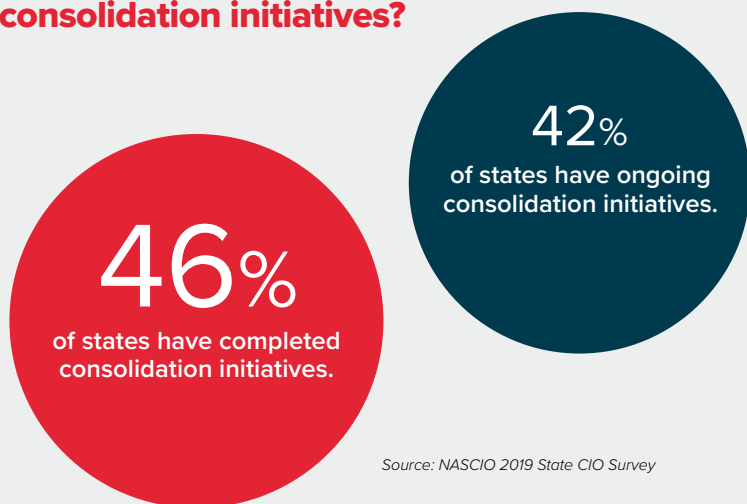
Source: NASCIO 2019 State CIO Survey

EMBRACING THE CLOUD

Succeeding with digital government requires agencies to embrace emerging technologies, including the cloud. However, many government IT organizations still rely on on-premises data centers or a mix of on-premises and cloud environments.

According to a 2019 Center for Digital Government (CDG) survey, 40 percent of government leaders said their agencies had adopted hybrid cloud environments. These leaders said 37 percent of their workloads were currently in the cloud, but up to 65 percent of their workloads could ultimately be handled using cloud solutions.

"Government agencies have this pressure to move to the cloud. They're running their own data centers or outsourcing the running of their data centers to a third party. By using the cloud, they see economic savings, but it's also a new way of doing things and they're not exactly sure how to get there," says David Egts, Chief Technologist, North America Public Sector at Red Hat.

40% of state and local government agencies have adopted hybrid cloud environments.

These agency leaders say **37%** of their workloads are in the cloud.

But **65%** of their workloads could ultimately be handled with cloud solutions.

Source: 2019 Center for Digital Government survey

"Government agencies have this pressure to move to the cloud. They're running their own data centers or outsourcing the running of their data centers to a third party. By using the cloud, they see economic savings, but it's also a new way of doing things and they're not exactly sure how to get there."

– David Egts, Chief Technologist, North America Public Sector, Red Hat

Some state and local governments are finding ways to maximize the use of cloud technologies and services. Texas, for example, became the first state in the country to create a cloud services marketplace. The marketplace allows state agencies to purchase and deploy vetted public cloud solutions and adopt a hybrid cloud model. The marketplace allows Texas' state agencies to still control their IT environment with a private cloud, while taking advantage of cloud innovations without investing significant IT resources in maintaining these solutions.

Traditionally, government agencies have relied on one cloud provider or a small selection of vendors for their IT needs. However, to remain flexible, agencies should consider adopting a container platform that prevents vendor lock-in as they move to the cloud. Containers allow developers to package all the software components and dependendies of an application together and isolate it from other processes so the application can easily be run in different computing environments, whether it's on-premises, in the cloud or a hybrid environment.

A container platform allows government IT teams to deploy applications faster, giving agencies the freedom to innovate and implement emerging technologies without relying on the traditional big-bang

approach to development. Solutions like Red Hat OpenShift, a container platform that accommodates on-premises, hybrid and multi-cloud deployments, can help government agencies balance agility with security.

"Rather than relying on one cloud vendor's solution, OpenShift allows you to take your application, put it in containers and run it on one cloud environment. If you choose to move to another cloud environment tomorrow, it easily allows you to migrate those workloads," Egts says.

"OpenShift comes with a lot of technologies that allow government agencies to do things like data integration," DiMuzio says. "A big problem for most government agencies is that they have all these disparate data sources. There's data integration capabilities built into the platform, and at an enterprise level, agencies can do business rules management and API management."

DiMuzio adds that cloud-agnostic tools like OpenShift allow government agencies to access all the building blocks necessary to create and deploy critical business applications.

There are plenty of use cases for container platforms in the public sector. Government agencies can use a container platform to manage microservices and quickly deploy new

self-service tools that enable citizens to apply for a business permit or access real-time data about their water usage, for example. State and local government CIOs also can use this strategy to accelerate the development-to-production pipeline for internal applications that increase organizational efficiency, such as tools that streamline Medicaid eligibility determinations for health and human services departments or that enable data sharing across different social services programs to identify fraud or abuse.

Some agencies are already realizing some of these benefits. One Northeast agency, for example, is using Red Hat OpenShift to enable citizens to quickly apply for and receive benefits. The agency's modernization efforts allow it to make changes to its customer portal within days instead of months, delivering faster service and a better customer experience.

A state agency in the Southwest has used OpenShift to automatically scale resources to meet tax season demands and to ensure constituents have a

seamless filing experience. The state also has flexibility to move these workloads between on-premises data centers or cloud resources without service disruptions.

That's just the tipping point for how container platforms built on an open source, standard operating system can drive a DevSecOps approach that streamlines backend operations and improves collaboration within IT organizations. With this approach, state and local government IT teams can accelerate application delivery while reducing IT complexity and costs.

"There are a lot of economies of scale because you don't need to retrain many of your people on a new cloud platform," Egts says. "The testing cycle is a lot shorter because you have a lot of commonality."

As government agencies modernize their IT infrastructures, enterprise open source technologies like a container platform can help them extend their IT capacity and leverage cloud resources to meet citizen demand for better service. »

FOCUSING ON DATA MANAGEMENT & ANALYTICS

One of the biggest challenges for state and local governments is harnessing all the data they collect and transforming this information into insights that improve service delivery.

However, the data government agencies collect — which includes everything from financial and operational data to de-identified data from health and human services programs, contract data for various vendors and personally identifiable information (PII) such as Social Security numbers and email addresses — is often stored in many disparate places. All this data might be scattered across public and private cloud environments, within on-premises data centers, and unfortunately, on paper.

Although government agencies must become more data-driven, they must also operate within a landscape that is increasingly privacy and security-focused, as recent laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act demonstrate. Though these regulations affect the private sector, the public sector also must be extremely diligent about how it collects, uses and manages data.

CDG research indicates CIOs are keenly aware of the challenges they face with using data as a powerful strategic tool while safeguarding this information. In a CDG survey of state and local government CIOs, 25 percent said data management and analytics was a key focus of strategic planning within their organizations, while the same percentage also said it was a top challenge.

Better data management is both an opportunity and an obstacle for government agencies. Successfully navigating this challenge can reap several long-term benefits for the public sector. Data analytics and data-driven open source solutions can reduce manual work for employees, free them to focus on high-value business needs, streamline federal and state compliance requirements, and uncover business insights that improve program performance and program quality.

To fully capitalize on data management and analytics, government agencies must adopt a holistic approach that focuses on these priorities:

■ **Data architecture and data governance:** Agencies must employ principles, practices and tools that ensure data quality and data security. They must create a framework for when, where and how employees in their organizations use data to drive value and improve service delivery.

- **Data strategy:** In collaboration with other business units and key stakeholders, state and local CIOs must create an action plan to use data as a strategic asset. This should align with their technology procurement and modernization strategy, as well as their overall mission and individual program goals.

- **Big data:** Government IT organizations must harness the vast amount of data agencies collect to improve program performance and introduce new citizen services.

- **Business intelligence:** Data from disparate resources should be shared, integrated and transformed into insights that drive action.

- **Predictive analytics:** Government agencies should be able to uncover patterns and trends that lead to improved forecasting and strategic planning and that moves their organizations toward more proactive, data-driven decision-making.

Better data management and predictive analytics can help government organizations mine insights from their data and drive more business value. In many parts of the country, data is already producing positive outcomes.

One Southeast government agency is using data to drive operational efficiencies and cost savings. The agency, which is responsible for managing electric utilities and regional economic development, implemented Red Hat Insights to predict and report system issues before they caused unplanned downtime. This is just one example of how predictive analytics can help government organizations proactively respond to incidents that can affect security, system performance and public services.

Other government agencies use data to improve public safety, emergency management and transportation planning. One of the largest counties on the West Coast used open source solutions to deliver key information to citizens during wildfires by autoscaling to accommodate an unprecedented deluge of website visits, ultimately helping to keep many residents safe.

Additionally, several municipalities are transforming themselves into smart cities, using open source technologies to create data-driven applications that improve their transportation systems, reduce traffic congestion and make their roadways safer. In the Northeast, a transportation authority has used open source solutions to build a mobile app that enables proactive rail maintenance and better asset tracking.

Data also can be beneficial for health and human services programs. A major state government in the Midwest used Red Hat OpenShift to deliver more responsive services to residents who receive benefits from SNAP, TANF and child support programs. Other local and state agencies use analytics to map opioid hotspots, track overdoses and identify high-risk groups that could benefit from early intervention programs.

By leveraging strategies and technologies that streamline data management, government agencies will be better positioned to advance their data capabilities. They then can take advantage of analytics to augment employees' skills and capabilities, creating more capacity to drive innovation and achieve long-term strategic goals. »

BUILDING A FOUNDATION **FOR** DIGITAL GOVERNMENT

As Egts says, "Innovation does no good if you can't secure it."

As governments become more nimble and more digitally enabled, cybersecurity and risk management are critical. This is a key focus for state and local government CIOs in 2020.

As of 2019, 62 percent of public sector organizations had experienced at least two cyber attacks in the previous two years. As state and local governments become more susceptible to these threats, security and privacy by design must be non-negotiable as part of the IT innovation process. Government

agencies must adopt solutions with integrated security standards and features, and must establish an enterprise-wide cybersecurity program focused on technology, training and vendor management to combat evolving security threats.

Here are some ways they can approach this:

TECHNOLOGY
Standardized environments offer more security.

"With standardization, there's a lot of commonality in your security profile," Egts says. "Your attack surface in the cloud is very similar

62%

of public sector organizations had experienced at least two cyber attacks in the previous two years.

EMPLOYEE TRAINING

Just as some state and local governments provide innovation training to their employees, they also should invest in more robust cybersecurity training.

This training can take several forms, but some effective strategies include regular phishing tests and internal security audits that assess a range of security threats, including weak or exposed passwords and bring-your-own-device policies.

Along with creating a culture of innovation, leaders must create a culture of cyber-awareness. Government organizations must continually test — and re-test — employees' knowledge as the threat landscape evolves. Taking these measures, along with incorporating modern technologies that integrate the most-up-to-date security protocols, can help safeguard government systems and data.

VENDOR MANAGEMENT

While state and local governments can take meaningful steps to secure their own in-house systems, solutions from external vendors likely will underpin much of their IT infrastructures.

For this reason, it's critical for agencies to define their minimum acceptable security standards and use this criteria to assess vendors as part of the RFP process. Agencies should gather information about each potential vendor's cybersecurity program and perform regular security audits with existing vendors to ensure these companies conduct proactive security and have updated incident response plans.

"Gone are the days when you just buy security tools. Now, the expectation for government agencies is that security is inherent in the product that they purchase. It should be secure by default," DiMuzio says. **»**

to on-premises. Instead of having two radically different security policies and multiple teams, you can have a single team that can make sure your systems and applications are secure no matter where they're deployed."

Container platforms can also help agencies build, deploy and manage applications securely. With vulnerability scanning and multi-tenant isolation, these platforms increase development without exposing critical systems to security risks.

Data classification policies and encryption standards are also key. State and local government agencies should work with strategic technology partners that certify their solutions in alignment with federal government standards, including Common Criteria, the NIST National Checklist, the DISA STIG and FIPS 140-2. Good data governance policies and practices and an ongoing plan for assessing the threat landscape (especially as new technologies are adopted) also should be core facets of an end-to-end cybersecurity program.

CONCLUSION

State and local governments face several challenges, including aging IT infrastructure, outdated processes and ongoing resource constraints.

Government must become more nimble. A DevSecOps approach and enterprise open source technologies can drive this transformation. By adopting best practices, processes and technology from the open source community, state and local agencies can move toward a standard operating environment, leverage the cloud and data analytics, introduce automation and create a modern IT infrastructure that helps them evolve into digital government.

Innovation is an ongoing process, but it's now non-negotiable for the public sector. To achieve their missions, state and local governments must prepare for and embrace technology disruption. Their ability to meet the needs of their constituents depends on it. »

ENDNOTES

1. https://www.redhat.com/en/services/consulting/open innovation-labs

2. https://www.impactmapping.org/

3. https://www.redhat.com/en/about/press-releases/red-hat-collaborates-unicef-innovation-accelerate-big-data-social-good

4. https://www.datacenter knowledge.com/business/after-decade-data-center-consolidation-us-states-report-mixed-success &
   https://www.nascio.org/resource-center/resources/shrinking-state-data-centers-a-playbook-for-enterprise-data-center-consolidation/

5. https://www.govtech.com/computing/Navigating-the-Road-to-Consolidation.html

6. https://www.redhat.com/cms/managed-files/li-enterprise-linux-server-datasheet-f11191jm- 201803-en_2.pdf

7. https://static.tenable.com/marketing/whitepapers/Whitepaper-Cybersecurity_in_Public_Sector.pdf

8. https://gcn.com/articles/2019/10/10/hybrid-cloud-state-local-gov.aspx

9. https://statetechmagazine.com/article/2018/09/hybrid-cloud-boosts-enterprise-agility-state-and-local-governments-perfcon

10. 2017 Red Hat Ebook, "Navigating Government's Digital Transformation: How a Focus on Values Drives CIO Technology Priorities," pg. 5.

11. 2017 Red Hat Ebook, "Navigating Government's Digital Transformation: How a Focus on Values Drives CIO Technology Priorities," pg. 5.

12. https://static.tenable.com/marketing/whitepapers/Whitepaper-Cybersecurity_in_Public_Sector.pdf

13. https://access.redhat.com/articles/2918071

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Red Hat.

Produced by:

TD SYNNEX
Public Sector

For:

Red Hat

State and local government agencies demand performance, transparency, and value—exactly what Red Hat offers. As the standard for Linux in governments worldwide, our cloud, virtualization, storage and platform solutions bring freedom and collaboration to the public sector. Bring the power of open source to your agency.

We are a part of a larger community working together to drive innovation. Learn more at: **www.redhat.com/government**