

SOLUTION NOTE

UNIFIED NETWORKING AND SECURITY FOR MORE EFFICIENT GOVERNMENT, FOR THE PEOPLE

THE PUBLIC SECTOR: STATE OF THE UNION

The COVID-19 pandemic forced state and local governments to reduce expenses. State and local budget shortfalls were estimated to run from \$500 billion to over \$900 billion in 2020. Those government budgets are just now recovering in 2021 with support from new federal rescue plans that will contribute billions of dollars to state and local governments. This support will expand initiatives in education, vaccination and testing and add over 100,000 new public health jobs.

In 2021, the pandemic's impact continues to drive increasing requirements for digital infrastructure and modernization. Workplace social distancing and masks will remain in place, likely for most of 2021, and these requirements will impact physical office locations and internal infrastructure.

Most important has been the need for deploying and managing secure work from anywhere (WFA) environments. The "new normal" shows us that WFA will continue, perhaps long after the pandemic, for non-essential functions. Organizations and technology supporting WFA continue to be re-engineered to meet new requirements more securely and at a lower cost. Fiscal reality and new budgetary constraints are driving innovation and efficiency where policy must be rethought and reformed to match reality and human behavior.

The Public Sector Moves Forward

The days of long lines at public service locations are almost over. The public is tech-savvy and has gone digital. Every patient has an electronic record; every student has a Chromebook or an iPad. Citizens and employees want to interact with the government from anywhere. The speed at which constituents are moving is creating a need for the public sector to modernize and transform its networks to meet new priorities.

PUBLIC SECTOR PRIORITIES

Public sector priorities continue to drive requirements for technology-based initiatives that require modernization and transformation. State spending before 2020 showed annualized budget increases with common priorities including cybersecurity, cloud computing, addressing personnel and talent gap issues, leveraging data analytics and improving connectivity with 5G. Election security will also continue to receive substantial attention.

State and Local Government IT

- Work from anywhere
- Smart cities
- Operational efficiency
- Citizen engagement
- Interagency collaboration and data sharing
- Governance and compliance
- Business process optimization and automation

Public Health

- Vaccine distribution
- COVID-19 testing
- Contact tracing requiring new infrastructure everywhere
- Patient communications
- Cybersecurity for standard and non-standard medical devices
- Telehealth and virtual care from anywhere

Education

- Distance learning: learn from anywhere
- Cybersecurity: BYOD, IoT
- Student safety to ensure both physical and online safe browsing experience
- Bandwidth and connectivity

IT MODERNIZATION AND TRANSFORMATION

Modernization is necessary to support such priorities and the technology-based initiatives they require. For example, securing and protecting a wide variety of Internet of Things (IoT) devices is key because most technology-based initiatives use these devices.

Network challenges require support for both hybrid and multi-cloud infrastructures in state and local government organizations. Information technology teams require deep visibility into all assets and need to manage these assets efficiently at any scale. Automation of IT service management workflow and related applications is essential to supporting this modernization.

Security challenges have increased substantially because of the move to the cloud, increased vulnerability and exposure of WFA environments, rapidly expanded use of mobile devices, and necessary support for hybrid environments. These issues have brought an expanded attack surface, a more complex threat landscape, severely over-burdened security operations center (SOC) and IT teams and new requirements to detect threats and remediate them at increasing levels of scale.

INFOBLOX FOR THE PUBLIC SECTOR

Infoblox Benefits

Infoblox can help meet your modernization requirements for secure, resilient and flexible network core services and DNS security—including reaching 100 percent business continuity, preventing unplanned expenses related to breaches and protecting the public trust.

Our solutions help IT and SOC teams maintain important compliance over people, devices and the systems they use, improving operational efficiencies and driving deeper interdepartmental visibility and data integrity.

Infoblox Technology Solutions



DDI (DNS, DHCP & IPAM)

Deliver business-critical
network services



Network Service & Protocol Delivery (DDI)

- Core Network Services
- Application Load Balancing (DTC)
- Reporting
- Configuration Management
- DoT/DoH



Security

Protect the organization in
new threat landscape



Foundational Security Everywhere

- Visibility and discovery
- Detect and block malware, data exfiltration
- Threat Intelligence Optimization
- Security Automation and Orchestration, SOC efficiencies

Infoblox is the industry-leading provider of DNS, DHCP and IPAM (DDI) services, meeting the needs of any enterprise architecture, with appliance-based or SaaS-delivered solutions built for performance, scalability, security and reliability.

BloxOne® Threat Defense is Infoblox's hybrid security offering that strengthens and optimizes your security posture from the foundation up, using DNS as the first line of defense. It detects and blocks malware C&C and data exfiltration, and it leverages the data within DDI to enhance your entire cybersecurity ecosystem. BloxOne Threat Defense protects IoT devices and helps secure on-premises, cloud and hybrid environments and the WFA users who access them.

Infoblox Public Sector Cloud Program

Infoblox is proud to be the only secure DNS, DHCP and IPAM (DDI) vendor to be supported across all Public Sector AWS cloud instances (Commercial, FedRAMP High Govcloud, and the Top Secret C2S) as well as across both Microsoft Azure Commercial and Azure for US Government clouds. This gives our Public Sector customers the flexibility to deploy Secure DDI services in a multi-cloud environment allowing for unparalleled reliability and security with the ability to take advantage of FedRAMP secured cloud instances.



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com