carahsoft

infoblox

Advancing Federal Cyber Resilience

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V, GSA 2GIT, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Infoblox, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/infoblox-resources

Join Events & Webinars:
carah.io/infoblox-events

Discover Technology Solutions:
carah.io/InfobloxOverview

Learn About Procurement:
carah.io/infoblox-contracts

Connect With Our Team:
Infoblox@carahsoft.com
(844) 985-0577

infoblox | carahsoft

Advancing Federal Cyber Resilience

Strengthening Mission-Ready Cyber Defense with Actionable Threat Intelligence

Federal cyber resilience requires more than strategy. It requires practical architecture, trusted partnerships and the ability to translate policy, mandates and threat realities into measurable mission outcomes. And it requires operationalizing NIST principles as foundational controls for Zero Trust, incident response and mission resilience.

At the Advancing Federal Cyber Resilience leadership forum, Infoblox Federal and Carahsoft brought together Federal Systems Integrators, cybersecurity leaders, technical architects and program teams for a focused discussion on how Infoblox solutions help agencies improve real-time asset visibility, apply secure Protective DNS controls that prevent and preempt cyber attacks, and strengthen mission availability through designed resilience. Together, these capabilities advance Zero Trust execution and accelerate federal modernization.

This was not a vendor briefing. It was a working session designed to connect federal cyber priorities to real-world use cases, reference architectures, capture motions and delivery-ready solutions.

What We Covered

Federal Cyber Priorities Are Moving from Strategy to Execution

Federal agencies are advancing Zero Trust, Comply to Connect, cloud modernization, threat defense and resilience initiatives as AI adoption accelerates across attackers, defenders and users alike. At the same time, quantum readiness has moved from “around the corner” to the agency doorstep, making proper execution more important than ever.

That execution starts with fundamental cyber hygiene. Agencies need accurate, real-time visibility into users, devices, applications, cloud workloads and network activity across hybrid, cloud and mission environments. Infoblox helps deliver the visibility, accountability and control agencies need through secure network services, Protective DNS and threat intelligence — strengthening resilience and accelerating mission-ready modernization. Just as importantly, NIST has now mapped DNS security outcomes across the Cybersecurity Framework 2.0 lifecycle, reinforcing that DNS is not a niche control, but an enterprise resilience function.

How Infoblox Supports Zero Trust Execution

Zero Trust execution requires more than policy intent. Agencies need real-time visibility, trusted asset context, secure access controls and operational telemetry across users, devices, networks, applications and workloads.

Infoblox helps close that execution gap by providing the foundational visibility, control and Protective DNS capabilities needed to support core Zero Trust pillars. This includes the Secure DNS practices emphasized in NIST SP 800-81r3, the Secure DNS Deployment Guide, such as resilient DNS architecture, encrypted DNS protections, and telemetry that supports both enforcement and response.

Infoblox helps agencies:

- Identify connected devices, assets and cloud resources in real time
- Establish authoritative network and asset context to inform access and policy decisions
- Apply secure Protective DNS controls to prevent and preempt cyber attacks
- Support SOC, SIEM, SOAR, NAC and Zero Trust policy engines with actionable telemetry
- Improve coordination across security, network and operations teams
- Strengthen resilience and availability across hybrid, cloud and mission environments
- Extend DNS telemetry into digital forensics, threat hunting and incident response workflows

Protective DNS Helps Agencies Prevent Attacks Rather Than Respond

Federal networks need to detect and stop threats before they become incidents. Infoblox Threat Defense uses DNS-layer intelligence and analytics to help identify and block malicious infrastructure, command-and-control activity, phishing, malware, DNS tunneling and data exfiltration.

By acting at the DNS layer, Infoblox gives agencies and their integration partners a scalable way to reduce risk across users, devices, workloads, cloud environments and remote locations. By applying industry-leading DNS-focused and asset-correlated cyber threat intelligence via a robust policy engine. CISA, NSA, MS-ISAC, and partner nations around the world already recommend Protective DNS; and the updated NIST SP 800-81r3 guidance recommends implementation to support real-time threat disruption and incident response. More specifically, the guidance emphasizes blocking or redirecting harmful traffic in real time, delivering visibility into real-time and historical DNS query and response data, and correlating blocked activity with user and asset context to support digital forensics and incident response.

Infoblox UDDI Provides the Foundation for DoW's Comply-to-Connect

Comply-to-Connect (C2C) requires agencies to discover, identify, and assess the security readiness of every device against a defined standard before they're permitted access to the network. Today, many organizations that leverage legacy multifunction server-based DHCP services are challenged with implementing Comply-to-Connect because an accurate, real-time view of IP-enabled assets isn't available to kickstart the C2C assessment chain.

Infoblox provides the authoritative, real-time fabric that supports this mission by helping agencies:

- Discover and classify connected assets
- Maintain authoritative IPAM and DHCP data
- Identify unknown, unmanaged or non-compliant devices and endpoints whether on premises and in cloud environments
- Share device and network context with vulnerability scanners, NAC, CMDB, SIEM, SOAR and other security tools
- Support automated remediation and policy enforcement workflows
- Provide accurate and authoritative asset inventory for compliance and audit activities
- Correlate DNS activity with DHCP and IP address assignment data to improve attribution, auditability and incident reconstruction

Infoblox does not replace identity, NAC, CMDB, SIEM, edge firewalls, or endpoint tools. It strengthens them by providing the DNS, DHCP and IPAM context; those systems need to make better, more informed decisions. That authoritative context aligns closely with NIST SP 800-81r3's emphasis on using DNS and address assignment data not only for access decisions, but also for investigation and operational resilience.

Why This Matters for Federal Systems Integrators

Federal Systems Integrators (FSI) play a critical role in helping agencies modernize infrastructure, meet mandates, and deliver mission outcomes. Infoblox provides a practical, architecture-ready, capability-rich solution that can be integrated into federal proposals, modernization programs, and cyber resilience initiatives. That value is stronger when framed against NIST SP 800-81r3 as a recognized blueprint for Secure DNS, Protective DNS and resilient cyber architecture.

Key Takeaways

Asset Visibility comes first.
Agencies cannot secure, verify or automate what they cannot see. Infoblox's solutions provide essential visibility into what devices and assets are in the enterprise at any given moment as well as a historical address assignment record. That unified view of the network and historical address attribution are critical to both the Enterprise IT and Security teams' individual missions.

DDI supports mission resilience.
Modern DDI helps agencies improve availability, automate critical network services, reduce manual processes and strengthen hybrid and cloud operations.

Protective DNS reduces risk earlier.
Blocking malicious infrastructure at the DNS layer helps stop threats before users, devices or workloads connect to dangerous destinations.

Zero Trust depends on context.
Infoblox provides the asset, network and DNS context needed to support continuous verification, policy enforcement, and automated response.

NIST SP 800-81r3 provides the operational blueprint.
Agencies need DNS security that supports prevention, visibility, resilience and incident response — not just policy compliance.

FSI alignment matters.
Infoblox and Carahsoft helps partners align across capture, proposal, architecture and delivery to support active pursuits and improve federal mission outcomes.

For FSIs, Infoblox helps strengthen:

- Capture and proposal strategies
- Federal reference architectures
- Zero Trust and Comply-to-Connect solutions
- Cloud, hybrid and multi-cloud modernization programs
- Threat defense and Protective DNS use cases
- Network automation and operational resilience
- Mission-aligned cybersecurity outcomes
- Standards-based alignment to NIST CSF 2.0 and SP 800-81r3 outcomes

When integrated early into solution design, Infoblox can help FSIs improve technical credibility, strengthen differentiation and create clearer alignment between agency requirements and delivery execution.

Continue the Conversation

Infoblox Federal and Carahsoft are ready to work with Federal Systems Integrators and agency teams to identify where Infoblox solutions can strengthen cyber resilience, improve asset visibility, reduce mission risk and advance current and future federal initiatives.

Connect with us to discuss how Infoblox can help agencies:

- Improve real-time visibility across users, devices, applications, workloads and mission environments
- Support Zero Trust and Comply to Connect execution with trusted asset context
- Prevent and preempt cyber attacks before they disrupt mission operations
- Strengthen availability and resilience across hybrid and cloud environments
- Integrate Infoblox into active pursuits, proposals and modernization programs
- Align agency modernization and resilience initiatives to operational Secure DNS and Protective DNS principles reflected in NIST SP 800-81r3
- Support joint federal opportunities with Carahsoft

To schedule a follow-up discussion, contact your Infoblox Federal representative or the Carahsoft Infoblox team.

Main: (571) 662-3997 Infoblox@carahsoft.com

About Infoblox Federal

Infoblox unites networking, security and cloud through a Protective DDI platform that helps organizations improve visibility, automate critical network services and strengthen cyber resilience. For federal agencies and their partners, Infoblox provides foundational DNS, DHCP, IPAM, asset visibility and Protective DNS capabilities that support Zero Trust, Comply to Connect, threat defense, cloud modernization and mission assurance.

About Carahsoft

Carahsoft supports Infoblox Federal by helping government customers and partner organizations access the technologies, contracts and expertise needed to advance cybersecurity, modernization and mission outcomes.