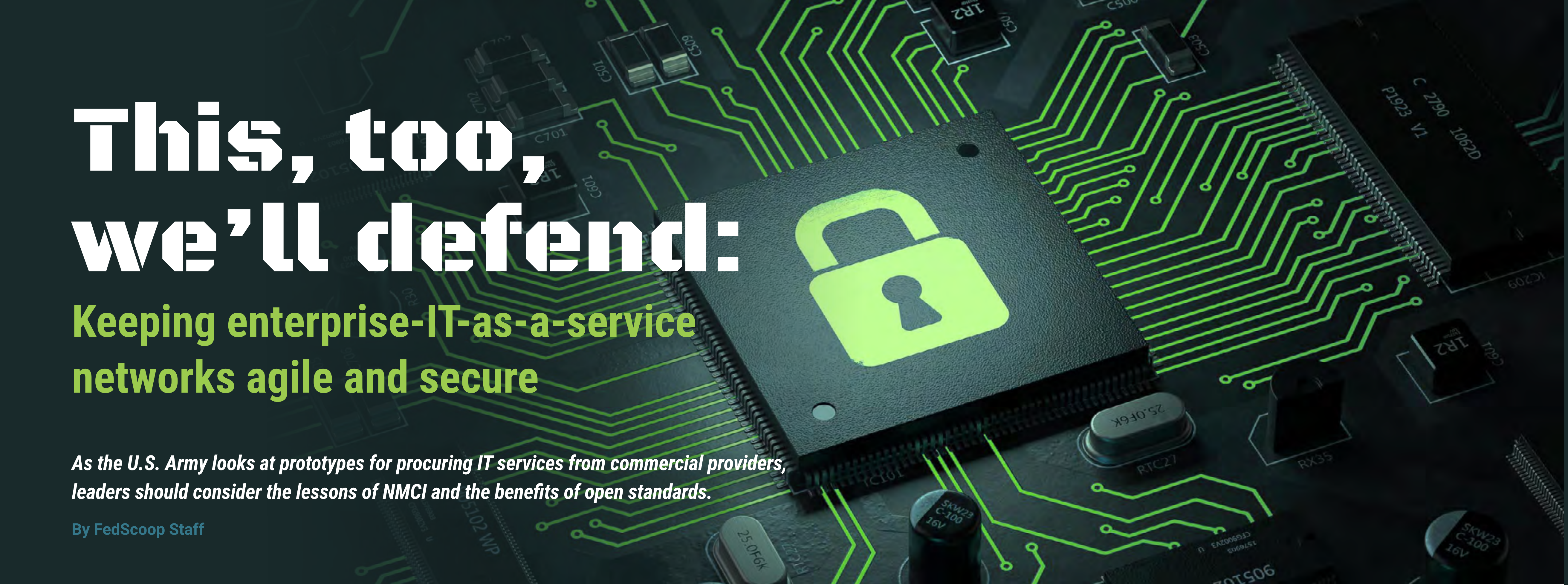


This, too, we'll defend:

Keeping enterprise-IT-as-a-service networks agile and secure

As the U.S. Army looks at prototypes for procuring IT services from commercial providers, leaders should consider the lessons of NMCI and the benefits of open standards.

By FedScoop Staff

As the U.S. Army, Navy and Air Force all embark on efforts to develop enterprise-IT-as-a-service models, they have two things going for them: the lessons learned from the Navy Marine Corps Intranet (NMCI) outsourcing program — and the ability today to adapt new technologies by working with vendors capable of leveraging open-source standards.

The ***Army's EITaaS initiative***, announced in March, represents the latest effort at the Department of Defense to shift the burden of managing the military's vast collection of IT systems to more agile and technically advanced commercial providers. It also stems from renewed convictions at the Pentagon that government-owned, government-operated IT systems are simply too slow to adapt and too costly to sustain to meet the military's future needs.

"We needed to do something fundamentally different," said Army CIO Lt. Gen. Bruce Crawford, summing up at a recent Army trade show what's driving broader plans to modernize DOD systems. "The Army's enterprise network at its current level of investment and current pace of modernization cannot meet the immediate and future warfighting requirements to optimize force readiness."

According to Crawford, 70 percent of the servers, routers and end-user devices in use at 288 of the Army's facilities worldwide — and 90 percent of equipment handling communications — are at or near the end of life. Replacing all of that gear would take until at least 2030, he said, and that doesn't fully account for the costs of maintaining all that legacy infrastructure in the interim.

Piloting new outsourcing models

Outsourcing the Army's enterprise IT services demands getting the right procurement models and service level agreements (SLA) in place. So the ***Army's EITaaS pilot program*** calls for commercial providers to provide prototype procurement models to deliver a wide range of foundational IT capabilities — including network infrastructure, end-user device provision, compute, storage and other cloud services.

The program mirrors similar initiatives announced last fall by the ***Navy*** and ***Air Force*** that have since led to multimillion-dollar contract awards. But it was also driven in part by meetings with leading private sector organizations, including Netflix and Airbnb. Those meetings gave Army officials greater appreciation for how to deliver innovative services to massive user groups while trusting commercial providers to handle backend network operations, according to Crawford.

They also informed three driving principles guiding the Army's IT plans, he said: Enable the Army to deliver IT at a commercial standard or better; continuously leverage industry best practices at scale; and optimize operations to better defend the Army network's mission systems and data.

Once the pilots are proven, the Army's goal, said Crawford, is to "move from an incremental approach at 288 different posts, camps and stations to more of a prioritized approach at about 50 of our most important and significant readiness-related, power-projection platforms."

Getting the foundation right

While Army officials hope to fast-track the prototype development process, utilizing a set of less-restrictive acquisition rules, they must still overcome various technical and cultural challenges, say DOD IT experts.

"One challenge we're seeing from our customer base, and the early prototypes at the Air Force, is shifting to a different acquisition mechanism — going from government-owned and government-operated to contractor-owned and contractor-operated [systems]," said Greg Bourdelais, who heads up DOD sales for Juniper

> **"Open source has never been more fundamental to technology innovation today forming the building blocks for widely used platforms in networks, clouds and applications in every industry sector.**
>
> – RANDY BIAS, VP, JUNIPER NETWORKS.

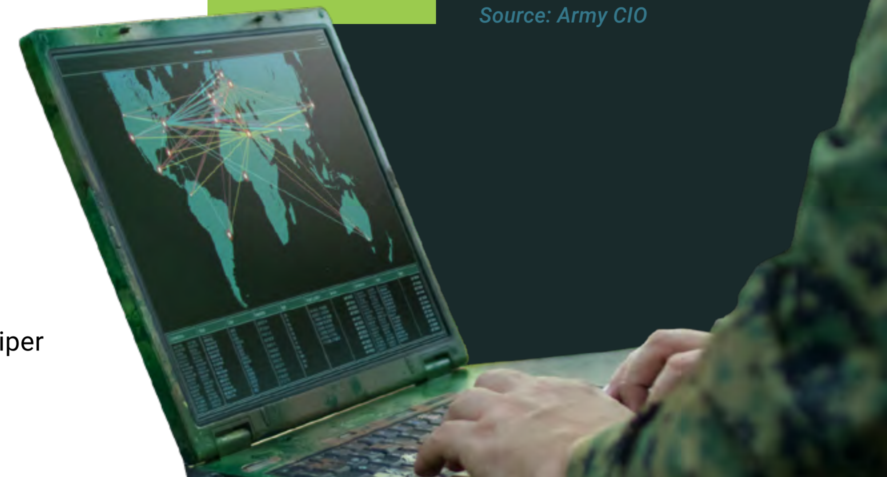
Army IT equipment at or near 'end of life' (Bases worldwide):

70% servers, routers & end-user devices

Source: Army CIO

90% communications equipment

Source: Army CIO



Networks. “Instead of acquiring a technology based on requirements, there are now going to be SLAs to support enterprise applications.”

Another concern is how to turn over the management of network infrastructure and services to third parties and still achieve pervasive visibility, security and control over essential operations, he says. Hammering out the provisions for network and system uptime and resiliency in SLAs is one thing; ensuring the agility and flexibility needed when units are deployed from garrison to the battlefield is another, noted Bourdelais.

A third, less obvious issue revolves around preserving room to innovate. Most contractors insist that they are committed to the DOD’s mission. But history suggests, when commercial contractors are in charge of the technology, government is “going to get a solution that pretty much just meets the requirements of the SLA — a box-for-box replacement. That can take away from the innovation that comes from looking at the full enterprise holistically, if you don’t write the SLAs properly,” said Bourdelais.

Those and other concerns, he said, argue for laying the right network architecture design principles in place at the outset — and being mindful about assembling commercial providers whose systems have proven ability to integrate and scale easily.

Lessons of NMCI

Many of those lessons were widely documented in the aftermath of the Navy’s bold and visionary decision 20 years ago to outsource and consolidate the management of almost 1,000 networks and 360,000 desktops into one seamless and secure intranet, sharing voice, video and data services.

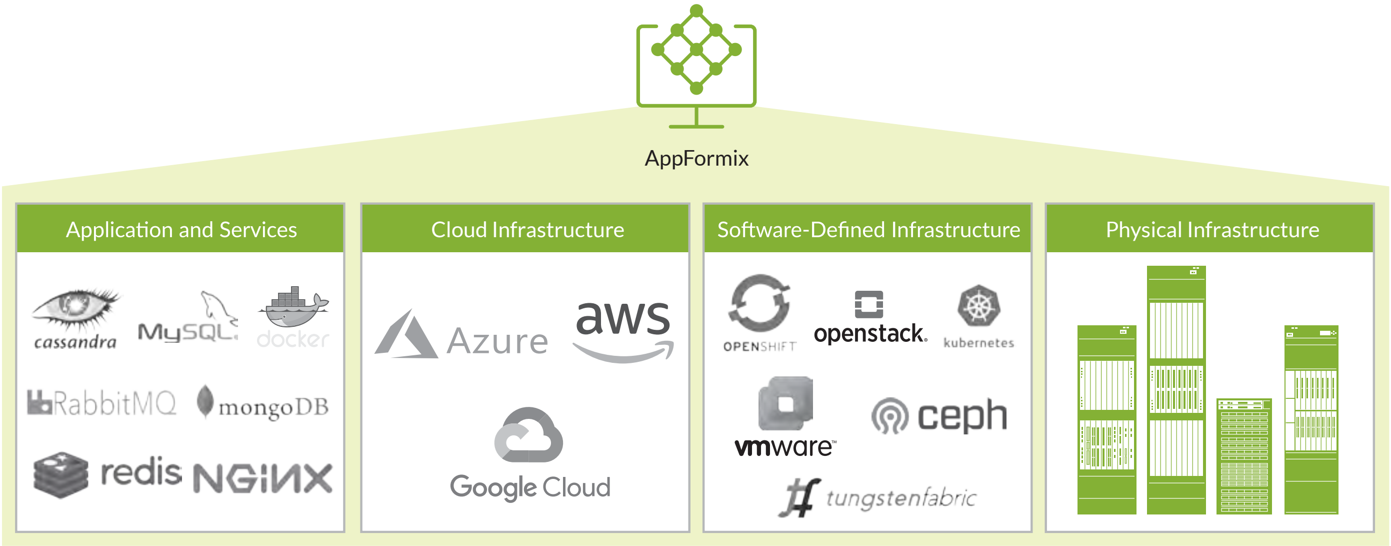
The scale and scope of the NMCI information network — second in size at the time to the internet itself — and its $8.8 billion performance-based contract with EDS were unprecedented in their day, according to an ***NMCI case study*** by the Center for Technology and National Security Policy at National Defense University.

The Navy succeeded in creating a single, standardized, enterprisewide computing and communications backbone that was also highly secure, if not always as fast as promised. NMCI was also notable for establishing performance-oriented SLAs linked to customer satisfaction targets. And it included provisions for NMCI to keep up with the rapid pace of technology, with minimum hardware and software refresh requirements.

But the NMCI program also exposed critical pitfalls to outsourcing, the study concluded:

- By choosing to use a single vendor, the Navy later found itself beholden to EDS’s IT choices, making it difficult and costly to transition to another vendor.
- Both the Navy and EDS failed to establish a realistic picture of the true number of applications and systems that needed to be transitioned.
- Inadequate steps were taken to implement and enforce user security policies.
- The SLAs turned out to be overly complex, difficult to manage and often lacked sufficient incentives to meet requirements.

> **The Army’s goal is to move from an incremental to more of a prioritized. [EITaaS] approach at 50 of our most significant readiness-related, power-projection platforms.**
>
> **– ARMY CIO LT. GEN. BRUCE CRAWFORD**



Juniper Network’s AppFormix gives network operators end-to-end visibility of both physical and virtual environments, using real-time monitoring and intent-based analytics.
Source: Juniper Networks

The case for open source and network visibility

One key step the Army, Navy and Air Force can take to ensure a healthier, more flexible framework for outsourcing IT resources is to work with vendors that embrace open source platforms, according to Bourdelais and others.

“Open source has never been more fundamental to technology innovation today, forming the building blocks for widely used platforms in networks, clouds and applications in every industry sector,” said ***Randy Bias***, founding member of OpenStack Foundation and now VP of Technology and Open Source Software at Juniper Networks.

“Leveraging open standards allows you to take advantage of the best of the best without being locked into a vendor,” added Mike Loefflad, systems engineering manager for federal accounts at Juniper Networks. It also supports a wider range of APIs for more seamless integrations between ***enterprise data centers*** and ***multicloud operating partners***.

Working with vendors that build on open source standards also assures greater agility as requirements change.

That’s increasingly true at the network infrastructure level, where open source software that can ***manage hardware functions*** is transforming the evolution of networking. New software-driven capabilities have spun up a whirlwind of product innovation, accelerated product lifecycles and lowered the cost of routing. That’s given network operators the ability, for instance, to scale horizontally, not just vertically, and exercise greater overall ***network security control*** across a multivendor ecosystem.

From a networking perspective, ***Bikash Koley***, chief technology officer and executive vice president at Juniper Networks suggests that even as organizations outsource the infrastructure to third parties, their CIOs still need to ensure there are governance and design principles in place to maintain overall management control. To that end, he recommends those design principles ***solve for five factors:***

- Multi-domain connectivity
- Multi-vendor orchestration
- End-to-end visibility
- Pervasive security
- Reduced complexity

All of which means EITaaS initiatives need to ensure the prototypes they develop aren’t just about delivering manageable SLAs — they also need to support a flexible, scalable, ever-evolving IT operating ecosystem that can adapt to the military’s future needs.

Learn more about how Juniper Networks — recognized as a “Leader” in Gartner’s 2019 Magic Quadrant for Data Center Networking — and its Contrail Enterprise Multicloud and Enterprise Data Center solutions can provide best of breed platforms to meet the military’s networking needs.

fedscoop JUNIPER NETWORKS