An AT&T Whitepaper

The Defense Network of Tomorrow—Today.

Six technology tenets driving the modernization of the DoD.

AT&T

Executive Summary

Military operations today are challenged by an uncertain and complex domestic and global environment. Advancing technology has fundamentally changed the nature of conflict. It is impossible to know the precise location or underlying mission of our country's next deployment, and nothing on the horizon suggests the future will be any less complex. Such an environment requires flexibility, agility, resilience and a broad portfolio of capabilities, not only for command and control of the forces, but also for the mission and business systems that support them.

Unfortunately, current systems at the Department of Defense (DoD) were designed for a more predictable past and are not up to the task of supporting the ever-changing present, much less an unknown future—and, as a result, are now under scrutiny. The current DoD infrastructure involves more than 15,000 classified and unclassified networks, connecting more than seven million computers and IT devices, 10,000+ operational systems in 770 data centers supported by a 170,000-person IT workforce.

It's a hardware-centric infrastructure, which almost all agree would never be built that way today, in light of the tremendous advances in network technology that have been made over the past decade. And it's not ready for future conflicts. Something has to change for American forces to retain decision-making superiority over potential adversaries.

But don't take our word for it:

> *"…The network the Army has is not the network it needs to confront the changing face of warfare."*
>
> Lt. Gen. Bruce Crawford, CIO, U.S. Army

> *"We can't buy new capabilities using old ways."*
>
> Air Force Vice Chief of Staff Gen. Stephen W. Wilson

> *"WIN-T currently is too fragile and vulnerable for potential conflicts against near-peer adversaries."*
>
> Chief of Staff of the Army Gen. Mark Milley

Addressing the concerns of these senior leaders demands a different approach. The DoD Network of the Future requires a move to Network-as-a-Service (NaaS). Such a move addresses the need to change the DoD acquisition strategy for its network from a build/operate/defend to an "as a Service" model. NaaS will deliver a network that is software-defined, orchestrated and cloud-enabled; leverages commercial carriers for the best level of modern security; and includes wireless technologies and embraces emerging Internet of Things (IoT) concepts. Networks can be deployed in minutes rather than weeks, and the cloud can be leveraged for secure VPN communications that never touch the public internet.

The key drivers for the DoD are the same drivers facing the rest of the federal government and commercial industry, i.e., leveraging data through predictive analytics, improving operational availability and supporting ubiquitous mobility, realigning personnel to higher value tasks, and driving out costs. Commercial network providers are already addressing these drivers. AT&T has invested $200 billion in its network over the past decade, leveraging the iconic AT&T Labs, and working across an extensive partner base to offer innovative solutions and world-class network service delivery. The Network of the Future already exists, and it's there to be leveraged by the DoD.

This is already happening in pockets. Maxwell Air Force Base in Montgomery, Alabama has been working with AT&T to improve base security and force protection using the latest technology. One of the first requirements was better perimeter integrity. AT&T installed infrared motion detection video cameras connected to both wireless and cellular networks, providing remote situational awareness. The system was integrated into the AT&T messaging toolkit, allowing alerts to go directly to handheld devices used on patrol.

Based on that success, the same kind of sensors have been integrated into many of the everyday operations of the base—gate monitoring, fleet management and energy consumption. Not only is security improved, but the cost savings are significant. By replacing specialized, proprietary hardware with software and virtualizing networking functions, it's estimated the Air Force can save $700 million on base networking services and $490 million on data transport costs—that amounts to $1.1 billion annually.

Having the DoD working more closely with AT&T would represent a "back to the future" relationship. There is a rich history of such collaboration—during World War II, AT&T perfected RADAR and SONAR to help defeat the Axis powers. During that conflict, the head of Bell Laboratories personally briefed the Joint Chiefs of Staff on how best to leverage such new and innovative technology.

Later, AT&T went on to invent the transistor and the UNIX programming language, which became the foundation of modern servers, workstations and mobile devices. In 1998, the AT&T network was designated as National Critical Infrastructure, and today it's the only approved service provider of the NSA Commercial Solutions for Classified (CSfC) program.

It's time the DoD leveraged this trusted partner again to transform its network. Moving to NaaS is a logical part the DoD Third Offset strategy, the quest to maintain a clear technological advantage over any potential adversary and increase lethality. For decades, American forces have possessed this advantage in every conflict. Today, the network is the platform that needs to support the projection of military capability around the world, and it needs to leverage proven commercial innovations to maintain that superiority while it simultaneously focuses its science and technology efforts on military unique capabilities.

AT&T is a 142-year-old institution that has a heritage of service to the American government. The company continuously reinvents itself to maintain its technology advantage at global scale, receiving an average of two new U.S. patents each business day. AT&T operates the largest and most modern network in the world, handling an estimated 197 petabytes of data per day. This network serves nearly all of the Fortune 1000.

The DoD should make better use of this foundational piece of critical national infrastructure.

Analysis and Recommendations

TODAY'S NETWORKING CHALLENGES

The DoD today still has analog, fixed, premises-based, time-division multiplexing (TDM) and even asynchronous transfer mode (ATM) infrastructure that drains billions of dollars in legacy operations and maintenance expenses from the DoD's annual budget, while unnecessarily exposing the DoD to cybersecurity risks. This aging network architecture is based on point-to-point circuits that require constant hardware maintenance and upgrades. In addition to not offering many features and capabilities of modern networking, these legacy technologies have long-term consequences such as a shrinking number of suppliers and limited ability to scale to meet evolving mission demands.

The current situation is partially a result of defense contracting, not network providers. The roughly 15,000 separate networks that comprise the DoD's network were built by hundreds of different companies that are not in the business of networking. Why should the DoD outsource the operation of networks to contractors whose networks are then managed by AT&T? The network transformation challenge faced by the DoD dwarfs that of any other organization in the world and needs to be addressed by a company that actually builds, operates and continually invests in networks on a global scale

Specific operational challenges include:

1. ***Increased cyber threats***—From 2013 to 2015, the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of Sept. 11, 2001. The increased volume and persistence of current and new threat actors make the current architecture vulnerable.

2. ***Network infrastructure efficiency***—While the current DoD backbone network achieves a 99.5 percent operational availability, higher availability is often required to effectively support enterprise voice, enterprise email, enterprise thin client, or the high availability, low latency, low jitter requirements of mission and weapons systems.

3. ***TDM systems supporting legacy C2 systems/applications***—While the military departments (MILDEPs) have multi-year strategies to migrate an aging and costly communications environment to a cost-effective collaboration environment, the existing TDM environment is 30 years behind current commercial technologies, and the DoD's recent methods of procuring MPLS and JRSS are already falling behind state of the art.

4. ***Aging infrastructure and limited capacity (CAT3 station wiring, power, HVAC, limited diversity)***—Outdated fixed installation infrastructure inhibits the DoD's ability to offer Internet Protocol (IP)-based services that enable enhanced communications, collaboration applications and enterprise services to all users.

5 *Interoperability within the DoD and between mission partners*—DoD enterprise maintains redundant, overlapping investments in internal and mission partner standards and interfaces, for interoperability and data sharing.

6 *Technology adoption/refresh and operationalization*—Equipment is nearing the end of useful life, requiring both refreshed and new technology to provide enhanced capabilities and continued network defense. Operationalization of tech adoption/refresh/modernization can take years to accomplish.

7 *Disparate NetOps/DCO models and NM/Cyber tools across DoD components*—Limited integration and automation make operations, administration, maintenance and provisioning (OAM&P) of the DoDIN labor intensive and complicated. The sheer number of the DoD individual help desks costs millions of dollars to staff, operate and maintain. For the most part, each desk conducts its functions in a similar manner. These help desks can be consolidated and augmented with digital labor, which allows personnel to focus on other mission areas.

8 *Complex and dynamic missions driving need for more agile and new capabilities*—Today's disaggregated, forward-edge missions are difficult to support with fixed networks. Warfighters demand networks and devices that are mobility-enabled and rapidly provisioned for specific mission sets.

9 *Next-generation end user devices/soft clients/mobility apps*—A significant number of DoD personnel work in non-deployable roles, performing tasks that require only basic office automation software and soft clients using Non-Secure Internet Protocol Router NETwork (NIPRNet)-connected desktops, notebook computers and mobile devices.

10 *Declining budgets—*Investments in new technologies and operational capabilities require a self-funding strategy for the department to stay within current budget constraints. Modernization or streamlining efforts would help to fund future year investments.

REQUIREMENTS

The DoD Network of the Future must be ubiquitous—available everywhere and "always on." History has shown the ability to communicate and share information is as important as ordnance, strategy and logistics to effectively support military campaigns. Today, there are often multiple active missions across the globe, making it imperative for distributed forces to be able to access information wherever they are, using various computing devices.

With nearly everything and every person connected to the network, a seamless information environment providing command and control that allows joint and coalition interoperability is critical to mission success. Therefore, it is essential that the DoD have the most modern Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities available.

Flexibility to handle growth is another requirement for the DoD Network of the Future. The DoD's current network architecture is incapable of handling growth, both in data requirements and reach. It is not ready to respond to changes in tasking, mission or partner composition with the requisite speed. While this is partially the result of policy decisions rooted in securing the technologies available at that time, acquisition and fielding decisions have cemented those policy decisions. The Network of the Future can break from those restrictions, providing an agile and responsive infrastructure without compromising security or integrity.

A more software-defined or controlled environment allows the network to scale out or scale up more quickly and enhances the ability to deploy the exact same service in diverse and distributed enclaves. Software supporting particular network functions (e.g., MPLS edge router functions) running on virtual machines allows network capacity to be efficiently augmented.

An "always on" network is more secure because all elements can be continuously updated or patched to address security vulnerabilities. DoD organizations can more easily "train as they will fight" by avoiding the time and effort required to stand up and tear down portions of the network when they need to train—and they always need to train.

Simplification and consistency are additional benefits of a software-based environment. Instead of bigger boxes, more virtual machines are added when scaling is needed.

The industry is moving to a more open architecture—moving away from a proprietary command line interface (CLI)-dependent provisioning model to a data-driven network model.

Such network transformation will deliver many immediate benefits to the DoD. These include:

- ***OpEx (Operations and Maintenance) Savings:*** The DoD will experience OpEx savings by reducing the number of times a technician has to visit an enclave location simply to change a network function.
- ***CapEx (Capital—Procurement) Savings:*** If all network functions can run on general purpose or commoditized hardware, the cost of the hardware is reduced.
- ***Growth:*** One of the biggest challenges to mission support infrastructure growth is the deployment of additional equipment for capacity, but that challenge should be significantly reduced if all of the hardware is the same.
- ***User Experience:*** Another potential benefit of NFV is that service could move to accommodate traffic. This could reduce the delay and increase the user experience.
- ***Reduced Time to Deploy:*** With all hardware the same, agencies can quickly test equipment and potentially deploy new capabilities faster.
- ***Expanded Vendor Ecosystem:*** Hardware independence allows smaller vendors to join the ecosystem, enabling the selection of best-in-breed vendors.
- ***Technology Integration:*** Since SDN has taken off in several networks such as LANs/WANs, NFV provides a virtualization platform for SDN, and can utilize OpenStack for its infrastructure.

For wide area networking (WAN), the DoD architecture already employs the use of commercial carrier transport. The use of traditional private line (OC-3/12/48/192) 2.4 to 10 Gbps layer 1 trunks has well known advantages and shortfalls. As AT&T and other common carriers move to newer infrastructure solutions, the DoD should look to adopt the solutions in a wholesale manner to leverage the commercial network provider's annual multibillion dollar investment in modernizing their networks.

Commercial network provider Layer 3 MPLS VPN offerings are secure solutions that are increasingly SDN-enabled and fully orchestrated. Commercial MPLS VPN offerings such as AT&T's VPN (AVPN) are built upon several security protection methods that make them as secure as the Layer 1, 2 and 3 technologies the DoD has used for many years.

THE ROAD AHEAD

There was a time when solving problems meant building the solution. You knew how to fix the network, because you built it. You knew the nuances of your IT, its quirks. The network was familiar and it worked. It worked really well, providing solid performance for a long time.

Then something changed. Technology became fluid, not solid. Innovation began to accelerate at an unforeseen and unprecedented pace. Software was the new kid on the block, and hardware became virtual. The model shifted from fix it to develop it. To keep up with the pace of modern IT, you need to lead—not build. Leveraging modern technology today takes allies and experts—allowing the DoD to strategize while providers develop and deploy.

For an example of transformative change, look at how virtualization fundamentally changed computer infrastructure, capacity and cost. Virtual machines exponentially increased the power and efficiency of servers, which then rippled out and changed how data centers were constructed.

This lead to the migration to cloud computing, and suddenly companies could build out their networks faster and at far less cost, while developing new products and services much quicker. It also enabled private industry to tackle the data center consolidation challenge years ago, an issue that continues to challenge government agencies.

These transformed networks truly change what's possible from a performance and flexibility standpoint. There is an expression well-known in IT and engineering circles—"faster, better or cheaper—you only get two out of the three." Today for the first time, software-based networks offer IT leaders all three aspects of the equation—greatly enhanced networking performance, speed to deployment and lower costs.

There are six main tenets that make this kind of network transformation a reality:

TENET 1

The Network of Tomorrow—Today

The past decade has seen the development of an innovation gap between commercial and government networks. The DoD is falling farther behind every year because of the accelerating rate of innovation in the commercial sector. With the government spending between 70 and 90 percent of IT budgets on maintaining legacy systems, there simply is no way for the DoD to keep up. This innovation gap is growing every single year and must be addressed.

Having the DoD increasingly look to commercial providers to help transform its network is a critical part of the Third Offset strategy, the quest to maintain a clear technological advantage over any potential adversary. Since World War II, American forces have possessed this advantage in every conflict. Today, the network is the platform that supports the projection of military capability around the world, and the DoD needs to leverage proven commercial innovations to maintain that superiority.

TENET 2

Network as a Service

Network as a Service (NaaS) is the best way for the DoD to adapt to and buy these dramatic IT market changes. NaaS offers the DoD a transformational and agile procurement solution, with industry best practices and processes honed over tens of thousands of federal government and global commercial engagements. For today's network, capabilities—rather than hardware—are purchased.

NaaS integrates infrastructure and operations—transforming networks to deliver high availability with reduced cost of ownership and a lifecycle support model that embraces technology innovations. NaaS provides a highly scalable and elastic model that will allow the DoD to deploy this solution globally.

NaaS is best implemented as a Contractor Owned Contractor Operated (COCO) model. Although managed services alone are a good match for some customers, a NaaS model provides the DoD with improved delivery, end user support and Life Cycle Management (LCM) of the network. This approach will unburden the DoD communications staff from many existing tasks, allowing them to focus on other areas such as mission defense teams.

Changing the DoD IT acquisition strategy is the key attribute of the NaaS model. Legacy strategies of short term, low price, technically acceptable (LPTA) procurements, as well as separate procurements for infrastructure and operations, inhibit the best-of-breed network delivery and innovation commercial network providers have mastered. Industry will invest and bring lower cost solutions to service contracts, if contract award decisions recognize the value of innovation and industry investment.

TENET 3

Software-defined Networking and Network Functions Virtualization

Software-defined Networking (SDN) and Network Functions Virtualization (NFV) are well-known, disruptive technologies that have been gaining in popularity in data center environments for several years and are now moving into the campus and WAN networks.

Industrywide, it's the overwhelming consensus amongst global network carriers to move to SDN/NFV rapidly, because the hardware-based alternatives lack the agility, security and reduced cost structures necessary for the commercial carriers to survive over the next two decades.

SDN involves the physical separation of the network control plane from the forwarding plane, with the control plane managing several devices. NFV virtualizes network functions that were performed by proprietary appliances onto commodity hardware. In existing DoD networks, switches, routers and other network devices are managed individually, with the focus on devices rather than applications.

SDN abstracts the control plane from individual devices, giving administrators the ability to view network flows end to end and optimize data traffic paths via policy. This provides freedom to systematically control the way data flows through the network. Doing supports automation and helps IT teams deliver new capabilities and services more quickly. This can make the DoD IT infrastructure faster, as near-peer potential adversaries look to close the IT gap with the U.S.

The basic idea with NFV is to take what has been learned from data center evolution and virtualization and apply that knowledge to the network infrastructure realm. In this way, the network becomes more like the cloud, giving the DoD the ability to share servers across the many network functions, such as load balancing, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), firewall and WAN acceleration functions. The server capacity can be shared for these network functions, just as it is in the data center. SDN/NFV is essential to strong cybersecurity.

As networking technology has advanced greatly over the past decade, so too has security. With legacy networks, the emphasis was on perimeter security, building a “moat” around your “castle” for keeping the bad guys out. As so many recent breaches have shown, perimeter defense alone is completely insufficient in the face of modern cyber threats. There is no set perimeter any longer. Virtualization allows for the separation of workloads, which can be secured independently and quickly spun up and torn down as needed.

Making this shift to SDN and NFV creates a new market for software, reduces reliance on proprietary hardware appliances and eliminates the associated life cycle costs. Much of today’s purpose-built hardware, such as routers and firewalls, will eventually go the way of phone booths and video stores. Organizations that fail to transform their networks eventually may no longer be able to purchase or maintain these devices.

TENET 4

Wide Area Networks—Wired and Wireless

There have been great advances in Comms-on-the-Move technology, and the DoD shouldn’t have to pay a high connectivity price for mobility. Prioritization and preemption can be built into mobile networks. A good example is FirstNet, the dedicated network being built by AT&T for public safety and first responder professionals in all 50 states and American territories.

FirstNet is operational today, years ahead of schedule, due to AT&T existing LTE network footprint. The evolved packet core (EPC) will be deployed in 2018, which will provide even more granular control to local safety organizations, leveraging spectrum set aside by the Federal Communications Commission. The EPC network will also provide first-of-its-kind security via end-to-end encryption of all communications and a 24/7, 365-day Network Operations Center.

As AT&T and other common carriers move to newer infrastructure solutions, it is important that the DoD actively begins leveraging the investments made by industry leaders to ensure it has the most modern communications capabilities available to support the warfighter. And as commercial network providers roll out new technology necessary, in a future where private line solutions are either obsolete or are carried over packet optical networks, it's also vital to partner with carriers to ensure that DoD-specific critical attributes are identified and provisioned.

Commercial network providers have broad ranges of protocols and technologies available to support the evolution of the DoD infrastructure and wide area network (WAN), while ensuring continuity of service during the transition for the DoD's critical applications and missions with high QoS requirements (in terms of data delivery rates, latency, jitter and availability, etc.)

AT&T uses various technologies to transport customer traffic at layers 1, 2, and 3. At layer 1, AT&T provides the next-generation layer 1 technology optical transport network (OTN), as industry migrates away from SONET.

AT&T supplies layer 2 transport with carrier Ethernet, such as services with AT&T's Switched Ethernet (ASE), as industry moves away from ATM and Frame Relay. And AT&T supports customers at layer 3 with the AT&T MPLS offering, AT&T Virtual Private Network (AVPN), as service providers use MPLS, which scales extremely well, in the core. AVPN is the flagship product that many other AT&T products and offerings use.

The existing size, scope, geographic footprint and quantity of DoD networks may make it impractical to initially use a single network technology. Therefore, a hybrid network solution may be the best option. Both Ethernet and AVPN services offer the DoD a range of choices and benefits that fill the need to run multiple applications at remote locations, bases, small depot sites and heavy bandwidth sites, such as data centers.

TENET 5
Cybersecurity

Data helps drive mission. Losing data to a malicious hack or leak can cripple the DoD's ability to effectively prosecute its mission. By employing technological advancements such as big data, machine learning and user behavior analytics, the DoD can enhance threat management capabilities to get ahead of cyber attackers.

A transformed network can learn from past attacks, find the behavior patterns between humans and machines that preceded the attack, and then search for patterns in current data. It couples this with the ability to make automated responses. In this way, attacks can be detected, stopped or mitigated prior to actual damage.

Machine learning is one technique that learns from the data and creates a model. Commercial network provider threat intellect and analysis capabilities will help the DoD detect, analyze and address security threats faster and more efficiently than ever before, by providing unparalleled visibility into data patterns and threat activity across the network.

The AT&T VPN Service (AVPN) is a Layer 3 MPLS that uses IP to deliver the attributes of a private network within the confines of a shared networking infrastructure. It allows users such as the DoD to build an application-aware VPN to link their locations and efficiently transport voice, data, and video over a single connection.

AVPN provides data transport that does not traverse the internet, mitigating all internet-centric vulnerabilities such as Distributed Denial of Service (DDoS) attacks. This technology enables the warfighter to collaborate and share information for heightened situational awareness, providing access to knowledge bases in which actionable information can be researched expeditiously across a secure, robust, private virtual cloud. AVPN also offers privacy (traffic isolation), QoS, and traffic engineering advantages, similar to those provided by a connection-oriented implementation, but without the complexity that former connection-oriented technologies imposed.

The highly redundant MPLS backbone supporting AVPN design delivers Service Level Agreements (SLAs) that support high network availability and AVPN characteristics enable DoD customers to position themselves for the implementation of the JRSS, which is also based on virtual route forwarding. This capability is identified in the Defense Information Systems Agency (DISA) Network Architecture Layer as converged IP/MPLS network and facilitates the DoD strategy of providing robust offerings in Infrastructure-as-a-Service and Software Defined Everything.

TENET 6

The Intra and Internet of Things

IoT refers the networking of physical assets that feature an IP address for internet connectivity and the communication between these objects with other devices and systems. Given the priority for the DoD to increase the use of sensors, IoT will be vital to meeting this objective.

Implementing IoT can mitigate the potential negative impact of budget constraints and personnel cutbacks. Without deploying personnel to visually track geographically dispersed and remote assets, federal agencies can monitor them from a central site—24 hours a day, 365 days a year. For example, IoT can help government organizations conserve energy, alert first responders to incidents, inspect critical infrastructure with sensors and record patient findings remotely, thanks to wearable devices. Even in these early days, it’s clear that the near real-time information and analytic capabilities provided by IoT technology can enable agencies to act quickly, streamline processes, be more productive and perform their missions more effectively.

The Department of Defense already uses IoT in combat, deploying millions of sensors to provide situational awareness to senior commanders and personnel on the ground, on the seas and in the air. The military uses radio-frequency ID (RFID) tags to track shipments and manage inventories between logistics hubs. It’s also testing case tracking for weapons transport.

Enterprises that have successfully introduced IoT deployments have followed variations of the following approach:

- Begin every IoT initiative with a comprehensive risk analysis and keep base line security access in mind.
- Isolate IoT data and networks into secure domains or enclaves from other IT systems and networks as much as possible.

- Help to secure the data both at rest on the endpoint where necessary and in transit (DaR/DiT) with industry compliant encryption cypher solutions (e.g., Advanced Encryption Standard (AES)-based and NIST FIPS 140 certified).
- Use existing security tools and controls when practical and integrate any IoT-specific security measures with the agency's overall security regime (e.g., DNS Server & Recursor protections).
- Select IoT endpoint devices that use standard protocols, permit software and firmware upgrades, provide on-board security controls and are manufactured by reliable OEM vendors with proper firmware, O/S and application Software Development Lifecycle (SDLC) practices.
- Get involved in relevant IoT-related standards activities. Verify that devices are certified by vendors and/or network providers to comply with new IoT standards.
- Ensure the proper alignment with solutions that meet agency standards and requirements. For example, does it require use of a FedRAMP-certified Software-as-a-Service or Storage-as-a-Service cloud?
- Leverage endpoint-to-network authentication and authorization standards to secure devices onto a wireless network.

Choosing the right provider is crucial for the DoD to realize the efficiencies, process improvements and other benefits of IoT. A good provider should offer services and platforms that cover the entire technology value chain, from devices and connectivity to platforms and applications. This will provide the tools and resources that free the services to focus attention on their mission, rather than dealing with the challenges of building IoT solutions for the first time.

It may seem as if the Internet of Things is just the latest technology fad, but the move to add sensing, diagnostic and communications capabilities to the tools used by IT professionals has been evolving over the past two decades. The DoD stands to gain significantly from IoT—from smart city/campus deployments to battlefield or operational field environments. A strategic approach to IoT security will help the military to more confidently begin pursuing IoT opportunities, while keeping potential risks in check.

SPECIFIC RECOMMENDATIONS

The accelerated speed of technological development requires changes in IT procurement policy. There are technologists inside the DoD who understand the direction, but there are bifurcated internal decision makers. The modernization vision is hampered when converted into rigid contracting requirements.

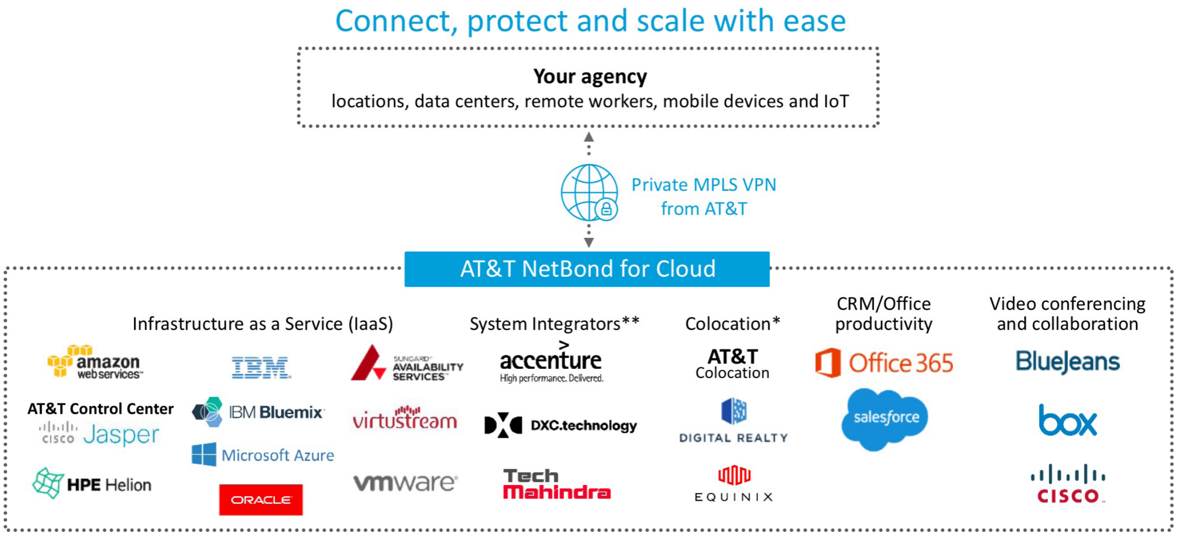
The government is challenged with procuring indefinite demand services, and has difficulty processing invoices that don't look the same every month. This is ironic, since years ago the government had no trouble with long-distance voice contracting, which of course was an on-demand service that billed the government only by how much was used.

While it's important that the DoD begin this transformative journey quickly, the journey itself is not a sprint, nor a "rip and replace" exercise.

Here are four specific ways to get started:

1 ***Take Advantage of Commercial Wired and Wireless WAN Capabilities (existing 1.0 imagery inserted for reference only)***
Make use of multiple next-generation DoD network capabilities in the context of a next generation WAN based on 1) MPLS VPN services, 2) Network on Demand (NoD), 3) AT&T FlexWare (NFV on Demand, and 4) AT&T NetBond cloud connectivity, Private Mobile Connections, and Commercial Solutions for Classified, demonstrating the applicability of new WAN technologies—wired and wireless—to the DoD environment.

The next-generation DoD network and protocol solutions developed could be used as the destination for flows sources in a private or government cloud. The next generation transport technologies tested will include SDN-enabled NoD, AT&T FlexWare and AT&T NetBond. An RFC-4364-compliant MPLS VPN service supporting six classes of service (CoS) would be used as the foundational transport.



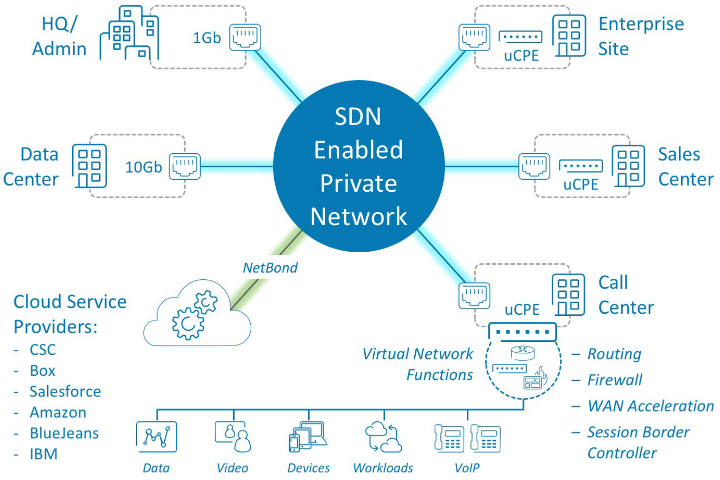
*Digital Realty & Equinix: 3rd party meet–me-point for Cloud Solution Providers only.
** System Integrators provide cloud transformation service and NetBond for Cloud to customers

AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are property of their respective owners.

This could then be expanded upon to demonstrate the capabilities of additional next generation transport technologies to include NoD, AT&T FlexWare, and AT&T NetBond, including Class-of-Service (CoS).

The DoD can gain additional insight regarding the interaction of network protocols and commercial service as they pertain to the separate enclaves and the emulated traffic flows.

Additionally, the DoD can become a fast follower of the commercial industry best practices that are "Mobile First" and "Cloud-enabled," without locking itself into single carrier or single cloud vendor solutions, both domestically and internationally.



- Ability to stand up new sites in days and add new services in minutes
- On-demand scaling of speed to support bandwidth-intensive apps (video, data replication)
- Multiple virtual functions on common hardware improving TCO
- Dynamic connection to mission critical user communities – e.g., provision VoIP seats in a call center on demand
- Easy to manage – software-controlled configuration and management

2 *Incorporate Commercial Security Products*

The DoD can leverage NFV to develop a security virtualization approach that supplements the current perimeter-based defense in-depth architecture to better protect DoD assets. Take advantage of commercial threat monitoring and logging along with Big Data capabilities to automate cyber incident management and analytics.

AT&T has some of the most sophisticated cyber defense tools and protocols in the world. By using the AT&T AVPN, the DoD can realize the benefits of these AVPN built-in security solutions. Offering multiple layers of security across applications, devices, networks and platforms reduces the risk of exposure from malicious attacks. AT&T has unparalleled visibility into potential threats as they try to enter its network. Using patented security analytics developed from decades of experience, AT&T proactively works to address identified threats before they reach DoD networks.

CYBERSECURITY SOLUTIONS

Threat Management

Helps to detect and respond to threats with 24x7x365 data monitoring and threat analysis conducted by a team of security experts.

- Deliver expertise, tools, and management to help mitigate risks posed by viruses, botnets, and advanced persistent threats
- Fortify protection with 24x7x365 data collection, monitoring, and analysis

Firewall Security

Designed to help prevent malicious threats from entering the DoD network and accessing critical data. These solutions also help:

- Defend the network against unauthorized connections and reduce risks of damaging attacks
- Provide expert management and 24x7x365 security monitoring
- Increase productivity by freeing resources to focus on mission-critical business

Web Security

Capabilities designed to help protect the DoD against threats that can enter its network through the internet. These solutions also help:

- Provide online filtering and control to help block malware and specific URLs
- Control web content and applications
- Provide proxy utilization and flexible configuration options through optional hybrid configuration

Security Incident and Event Management Solutions

Designed to analyze data across the network to correlate alerts and prioritize security events.

- Provides a broad view of network security by efficiently correlating alerts from multiple devices and device types
- Prioritizes security events based on threat and risk management methodologies
- Assists in helping to maintain compliance with government and industry regulations

3 *Exploit Mobility for IoT Capabilities*

The DoD can take important steps toward modernizing its networks by leveraging commercial network provider mobility and IoT capabilities.

It can do so and avoid costly infrastructure upgrades by leveraging LTE/4G mobility infrastructure and Smart Base capabilities to offer solutions to supplement (or even bypass) these challenges. As shown in the table on the next page, current Smart Base and IoT technologies can help the DoD meet several initiatives and comply with directives related to force protection, energy conservation, and vehicle maintenance and management.

AREA OF NEED	SOLUTION
Physical Security—Force Protection	Video Surveillance (motion & heat detection), Smart Fencing, Shot Spotter, Telemedicine
Energy Conservation	Smart Meters, Smart Grid, Smart Lighting, Vehicle Telematics, Smart Waste, Smart Water, Leak Detection, Water Quality
Vehicle Asset Management & Maintenance	Fleet Tracking and Telematics

4 ***Change the Way that DoD buys its Network***

DoD can accomplish a lot by exploiting two contracts awarded in 2017 by the General Services Administration (Enterprise Infrastructure Solutions) and the Department of Commerce (FirstNet).

EIS is a 15-year, $50 billion solution-based vehicle designed to address all aspects of federal agency IT telecommunications, infrastructure and modernization requirements. EIS can provide the services to meet immediate modernization goals today and continue to make technical innovations available, as those initial steps open new opportunities to the DoD.

For example, an initial modernization step might be moving all voice communications from TDM voice to IP infrastructure. This requires enhancements to VPN transport, managed infrastructure and equipment, and on-demand scaling. Once voice is handled by IP, many additional options emerge, such as unified communication services.

The FirstNet contract referenced earlier in the paper is also an excellent example of a more efficient way to purchase network capability. As the awardee of the FirstNet Program from the U.S. Department of Commerce, AT&T is providing a path of procurement for DoD customers to utilize FirstNet as a service via GSA Schedule 70 and the Army/Air Force blanket purchase agreement. Additional contract vehicles are in process.

The DoD can also leverage numerous contract vehicles from commercial providers to obtain a range of networking solutions.

Conclusion

The DoD needs a partner with global industry reach and influence that can provide highly assured connectivity and access. When the DoD is ready for the Network of the Future, it should talk to the company that handles one-third of global internet traffic and backs that up with a world-class network disaster recovery capability, as demonstrated in 2017 during our responses to numerous natural disasters in the US and the Caribbean.

AT&T has built the Network of the Future, today. The global network platform is 55 percent SDN today, and will be 70 percent by 2020. AT&T IT systems are over 80 percent virtualized today, and by 2020 over 50 percent of AT&T software will be open source. AT&T offers NFV services in 225 countries around the world, and the company recently released 8.5 million lines of code to support open source interoperability and innovation through the Linux Foundations Open Network Automation Project (ONAP, https://www.onap.org/).

Going with commercially-available network solutions provides the DoD operational, manpower, and resource benefits, as well as the opportunity to future-proof its network by leveraging Cloud, Mobility, SDN, NFV, and Orchestration services without vendor lock-in.

The critical nature of the national defense mission requires the DoD Network of the Future be bought (not built) as a best-in-breed embracing all of the innovations available in today's market. That's the best and fastest way to ensure its communications infrastructure meets the demands set by modern warfare doctrine.

AT&T Public Sector is on LinkedIn.

Join the conversation as we share stories of innovation, news and leadership across the Public Sector.

Click to follow