BROCADE

The Necessity for Network Modernization

A Roadmap to Mission Readiness

Agencies can leverage newer and more innovative networking technologies to enhance mission success. Networks are facing significant and evolving challenges that impact an agency's ability to deliver on mission objectives for citizens, first responders, warfighters, veterans, and others. The "New IP" is a series of new developments and technologies that can address the risks associated with outdated networks while delivering significant performance, cost, and security improvements. Closed networks stifle competition, hamper innovation and drive up costs. Transitioning to the New IP opens your network to innovation and increased capabilities. What if every soldier, law enforcement officer, or first responder could access critical intelligence in real-time when and where they need it? What if security was built into every network component and application, not just bolted on? What if you could scale up and down on demand, without cost penalties? What if you could do all this and save tax payers $7 billion over the next five years?

Over the last four years, this white paper was developed by conducting research, leveraging independent market research, and modeling the government's acquisition and use of Information Technology (IT)—to educate agencies on how to transform and modernize network infrastructure to improve IT effectiveness. This paper examines industry and market megatrends, financial drivers, technology innovations, the acquisition process, and proven methodologies required for the network transformation that will save billions of tax payer dollars and deliver improved government efficiencies. It will also discuss the challenges of the IT status quo and the leadership necessary to inspire change.

This paper will reveal how the risk of not modernizing, evolving, and transforming the network proves to be much greater than the costs associated with change. Industry insights and vision for today and tomorrow will demonstrate how these proven paths and concrete actions will enable the New IP, enhance IT effectiveness, and improve agency mission outcomes.

Table of Contents

A Roadmap to Mission Readiness 1

- Today's Technology Environment 3
- Market Drivers 3
- Financial Drivers 4
- Introducing the New IP 5
- Is Your Agency Ready for the New IP? 5
- What Is the New IP? 6
- Transitioning to the New IP 6
- Multivendor Solutions Promote Innovation and Accountability 8
- Leveraging Contracting to Increase Competition and Reduce Costs 8
- Emerging Technologies Require Open Standards 10
- Reduce Training, Maintenance, and Personnel Costs 11
- Software-Defined Networking Uses Open Protocols 11
- Fabrics are Evolutionary 12
- Embrace Innovative Technology 13
- SDN and Fabrics Provide Increased Network Security and Data Privacy 14
- Leverage Procurement Processes to Provide Limitless Upgradability and Scalability 15
- The Next Move 15

Today's Technology Environment

Everyone in government wants all the information needed to perform their mission at their fingertips, in real time. Personnel now expect to either consume or communicate this information through secure networks.

But agencies don't take anything for granted; IT and security pros are extremely aware of the risks that come with securing their IT and network infrastructures. They also know that the staggering number of network connected devices and vast amounts of data they are generating are taxing their outdated network infrastructures on a daily basis.

These decision makers also see the trends and their challenges. They have read the research from Gartner, Inc. which forecasted that, "4.9 billion connected 'things' will be in use in 2015 (up 30 percent from 2014). This number will reach 25 billion by 2020."[1] Others like Morgan Stanley believe this number can actually be as high as 75 billion connected devices, and believe that there are more new devices to come. They estimate there are 200 unique consumer devices or equipment that could be connected to the Internet that are not currently in use.[2] They know the demand for connected appliances will continue to challenge their network capabilities. And they realize to fulfill their daily mission; they have no choice but to invest in scalable, agile technologies that keep pace with relentless demand. Agencies recognize that today greater than 70 percent of every IT dollar spent is used to support legacy systems and they need to break that cycle to transform their IT environments. This fact is well documented in the report by the General Accounting Office (GAO), Information Technology: Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments.[3]

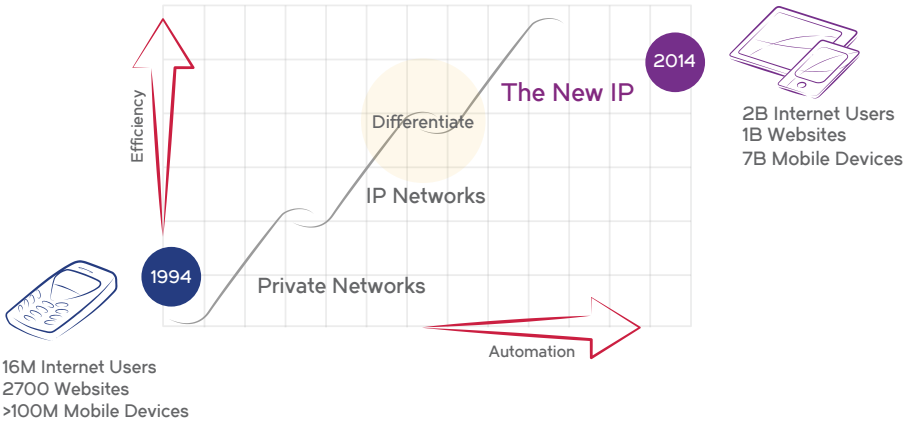
As agencies strive to evolve, transform, and modernize their networks, there are proven paths to success including:

1. Using multivendor networks as opposed to a single vendor network to continually introduce innovation
2. Mandating the use of open standards versus proprietary protocols to ensure interoperability and provide flexibility
3. Increasing competition to drive innovation and reduce costs
4. Leveraging innovations in the "Internet of things," mobility, cybersecurity, cloud, and Big Data
5. Integrating new solutions in networking coming from Cloud, Infrastructure as a Service (IaaS), Ethernet Fabrics, Network Functions Virtualization (NFV), Software-Defined Networking (SDN), and other technologies
6. Employing alternative acquisition models such as utility and "as a service"

Agencies realize they must leverage newer and more innovative networking technologies and acquisition models to enhance mission success; ones that are significantly more agile, innovative and secure; that provide a network infrastructure that is less complex and easier to manage; and ones that enhance mission outcomes, promote innovation and reduce overall costs through competition.

Market Drivers

"The Internet of Things (IoT)* has become a powerful force for business transformation; and its disruptive impact will be felt across all industries and all areas of society."[4] The technology industry tends to operate on micro and mega innovation cycles. Micro cycles happen every hour, day, week, and year. But mega cycles are far less frequent—about every 20 years. During these upheavals, there is a massive and fundamental disruption that changes not just the technology industry, but every other business and industry thanks to the far-reaching ripple effect. The upshot: Life on planet Earth gets impacted profoundly in terms of how we work, live, and play.



[1] http://www.gartner.com/newsroom/id/2905717

[2] http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10#ixzz3LJrl8jWN

[3] GAO-13-87: Published: Oct 16, 2012. Publicly Released: Nov 15, 2012

[4] http://www.gartner.com/newsroom/id/2905717

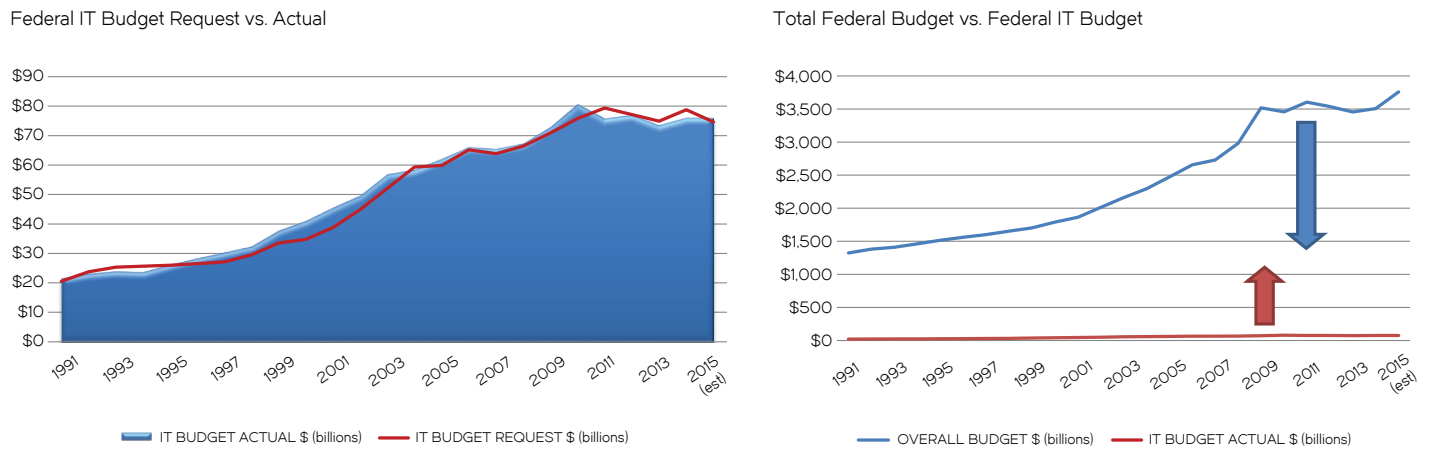


Figure 1: Table based on data available from OMB and Deltek.

In this new era, applications will become subordinate to user requirements and the information being shared, the distributed nature of information will drive the design and delivery of networks and network applications. Furthermore, the network must continuously evolve to meet the demands of the mission, enabling cloud computing, mobility, and the IoT while demonstrating greater flexibility, intelligence, automation, and security. Recently, the General Accounting Office (GAO) added Improving the Management of IT Acquisitions and Operations to the government's 2015 High Risk Report.[5] The network should be capable of leveraging policy-driven programming and virtualization to simplify management increase efficiency and reduce costs.

Security and privacy are also significant market drivers. Today, entire critical infrastructures are reliant on networks. Ever-increasing cyberattacks threaten national security and privacy. During recent testimony in a Hearing of the House (Select) Intelligence Committee on the subject of "Cybersecurity Threats: The Way Forward," the transcript stated, "The effects of an attack would send a shockwave through the economy. Remember how a single fallen tree in Ohio back in 2003 triggered a blackout for nearly 50 million people. Just think about what a cyberattack would do. It could be catastrophic."[6] The network must enhance security and privacy by employing embedded capabilities providing policy management, authentication, encryption, and continuous monitoring.

Transforming and modernizing the network further delivers on the government's policy mandates for sharing enterprise services, increasing efficiency and reducing acquisition costs. It promotes aligning costs with usage, accelerating innovation, and empowering mission solutions, not managing infrastructure.

Financial Drivers

While the Federal budget soars, the IT budget has remained relatively flat at approximately $80 billion annually, a mere two percent of federal spending. None the less, the Federal Government remains one of the world's largest enterprise consumers of IT solutions and services. As the size of government has increased, so have spending, mission responsibilities and the expectations for IT. Citizens, warfighters and veterans all have high expectations for improved and enhanced services from citizens' tax dollars and modern IT solutions. This escalating demand drives the immediate and ongoing need for network transformation to achieve greater efficiencies while keeping cost relatively constant. This is all in keeping with doing more for the same or less.

The "President's Management Agenda" lays the foundation for creating a 21st century digital government that delivers better results to citizens, warfighters, and veterans while improving the way digital services are delivered and serve the people. The agenda includes the efficient and effective acquisition of solutions that maximize the value of every taxpayer dollar invested in technology as it pursues the vision of building a "Digital Democracy."[7] The opportunity for savings through modernization of just the network

[5] http://www.gao.gov/products/GAO-15-290

[6] https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf

[7] https://cio.gov/delivering-customer-focused-government-smarter/

Potential Government Savings of $7 Billion
Leveraging Open Standards and Multivendor Networks

	($) Billion	Gartner 14.9% of Total IT Spend is Networking	Gartner 31% of Networking is HW & SW combined	Gartner 28% is Maintenance and Outsourcing	Gartner 41% is Staffing/ Personnel Support
Total Agency IT Spend	80.00	$11.92	$3.70	$3.34	$4.89

Networking Technology Segment	2015 IT Spend based on Exhibit 53 Data	Potential Savings (Min) 15%	Potential Savings (Max) 25%	Average Annual Potential Savings	Average Potential Savinngs over 5 years
Networking IT Equipment and Software (annual) 31% of Total Network Spend	$3.70	$0.55	$0.92	$0.74	$3.70
Maintenance Support Services and Software/HW updates (annual) 28% of Total Network Spend	$3.34	$0.50	$0.83	$0.67	$3.34
Staffing, Telecommunications and Network Services (annual) 41% of Total Network Spend	$4.89	$ —	$ —	$ —	$ —
Total Networking Spend (annual) 14.9% of IT Annual IT Spend	$11.92	$1.05	$1.76	**$1.41**	**$7.03**

Figure 2: Government Fiscal Year 2015 and Next Five Year's Estimated IT Network Spending and Potential Savings. Table based on Gartner's Total Cost of Infrastructure and Operations (TCIO) methodology and 15-25% estimated savings for introducing a second networking vendor.

Is Your Agency Ready for the New IP?

Is your network ready to support your agency mission five years from now? How about ten? If you can answer yes, unconditionally, to all eight of statements below, then your network is good to go for the next decade.

Your agency does extensive market research when developing requirements to the maximum extent practical.	YES	NO
Your agency requirements are linked to mission outcomes and defined in terms to desired features, functions, capabilities, and service levels to meet those outcomes.	YES	NO
Your agency networks are vendor-independent, using open industry standard protocols and restricting or limiting the use of proprietary protocols.	YES	NO
Your agency networks are agile and flexible, allowing you to quickly scale in or out and rapidly deploy new applications.	YES	NO
Your agency networks adequately protect and secure critical information, ensure data privacy today, and are prepared for the cyber threats of tomorrow.	YES	NO
Your agency networks are intelligent, automated, and simple to manage and administer.	YES	NO
Your agency networks are prepared for the explosive growth in mobility and the Internet of Things where everything is connected.	YES	NO
Your agency networks can be acquired as your needs warrant whether it be a capital purchase, lease, Infrastructure as a Service, cloud, or any combination.	YES	NO

If your agency answered NO to one or more questions, read on to learn how your agency can become ready for the New IP.

alone is astonishing. Figure 2 based on Gartner's Total Cost of Infrastructure and Operations (TCIO) illustrates how competition through multivendor versus single vendor networks could save the government over a billion dollars annually.

Introducing the New IP

The IoT demands a new, more agile and secure network- the New IP. The New IP is built on networking that is application-aware, allowing automation, control, simplification, and agility by using open Application Programming Interfaces (APIs) between layers and components.

The New IP is a highly innovative and advanced network, exploiting open standards and incorporating self-learning fabrics to remove complexity while simplifying management. Over time, all eras of computing (including the mainframe and client/server eras) have led to new networking paradigms and technologies. Today, the cloud and mobile era are fundamentally changing the industry, driving advancements across all aspects of IT. As a result, a new networking paradigm, known across the industry as the New IP, is emerging. The primary objective is a network that helps organizations tap into the unlimited possibilities of cloud, mobile, social, and Big Data. It will aid agencies in their quest to close the relevancy gap, improving the efficiency of IT and enhancing the services provided.

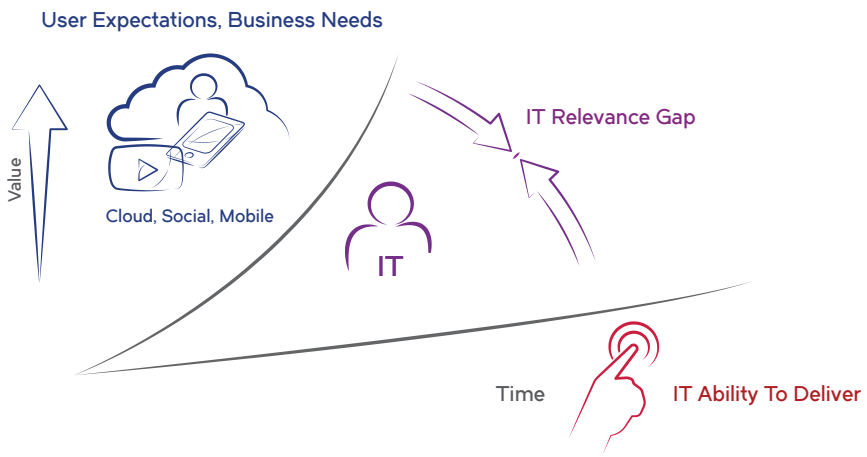


Figure 3: Close the IT Relevance Gap: Transform your IT department into a trusted provider of services.

What Is the New IP?

The New IP is a series of new developments and technologies that transition traditional networks from a "plumbing"-like approach based on proprietary hardware, manual configuration, limited flexibility, and high cost, to an intelligent network that is software-centric and a highly virtualized environment. It offers dramatically better scalability, flexibility, innovation, automation, adaptability, and control by leveraging open systems, programmability, embedded policy and intelligence, using open commercial off-the-shelf (COTS) hardware. The New IP allows the network to become tightly coupled and responsive to the applications and data that it serves, resulting in networks that are optimized, dynamic, and aware, and includes technologies such as SDN and NFV.

According to Gartner,[8] the density of legacy technologies in government is hampering CIOs' efforts to digitize their organizations. To demonstrate "digital now, digital first" leadership in government, CIOs must flip their approach to managing IT from the inside-out perspective of legacy constraints to the outside-in view of citizen experience.

The New IP is a result of the industry's recognition that traditional networks and acquisition practices inhibit organizations from achieving the unlimited possibilities of the cloud. The New IP represents a fundamental change in mindset about the role of networking and its ability to support the massive scale of today's powerful compute models.

To efficiently support government functions, the federal IT network must change—transitioning from traditional hardware-centric, proprietary architectures to an open, multivendor, software-centric New IP network. The New IP addresses critical business and technology challenges by helping agencies:

- Evolve their networks to fully leverage the unlimited possibilities of cloud, mobile, and social advancements to ensure mission success
- Accelerate the journey to the cloud, strengthen cybersecurity initiatives, ease the impact of data center consolidation, and deliver robust data analytics on any device, anywhere, anytime
- Increase flexibility and expand options using open solutions from a broad ecosystem of vendors and innovators
- Regain control over their networks, turning them into true business enablers that can quickly adapt to the changing needs of federal employees, citizens, and warfighters

Transitioning to the New IP

It is important to remember that the New IP is still a relatively new concept to many. Although the transition to the New IP is still in its early stages, the adoption of enabling technologies is already underway and rapidly increasing. Agencies can transition to the New IP incrementally, as needs direct and budgets permit.

Transitioning to the New IP is best accomplished through the following initiatives:

- **Implement a multivendor network:** Multivendor networks enable the competition that controls costs and encourages the use of best-of-breed products. The introduction of a second vendor into the network reduces the total cost of ownership by 15 to 25 percent over a five-year period.[9]

[8] Gartner, Inc. "2015 CIO Agenda: A Government Perspective," Jan. 30, 2015.

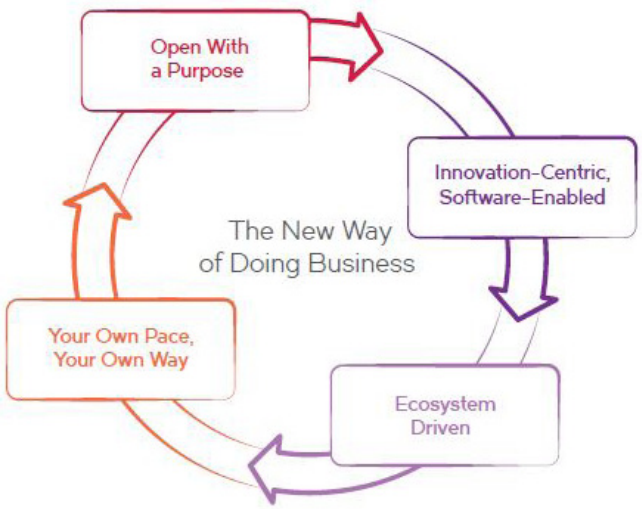
[9] Gartner, "Debunking the Myth of the Single-Vendor Network," November 2010.

- **Move to open standards:** By reducing vendor lock-in, standards-based products enable choice that increases flexibility while reducing cost and complexity. These benefits help accelerate the rate of innovation. Agencies that take advantage of open standards are more agile and better positioned to adapt to advances such as SDN.
- **Virtualize using NFV and SDN:** Begin using software-based technologies such as SDN and NFV to provide the dynamic delivery of new applications and services in minutes instead of days or weeks. NFV moves network functions from special purpose hardware devices to "common, off-the-shelf" servers to dramatically reduce IT costs. SDN is an approach to using open protocols, such as OpenFlow, to apply globally-aware software control from edge to core network devices that traditionally use closed and proprietary firmware. The freedom to programmatically control the way data flows through a network eases manageability, supports automation, and helps administrators more quickly deliver customized services that enhance agency operations.
- **Deploy Ethernet fabrics:** A fabric is a flattened architecture that simplifies networks by replacing traditional point-to-point relationships. Fabrics are extremely easy to deploy with a simple plug-and-play procedure. They are self-provisioning and self-healing, which eases scalability and dramatically reduces training and maintenance costs. Fabrics also feature automation that reduces errors and accepts commands and controls from enterprise-level orchestration tools such as OpenStack.
- **Leverage alternative utility and procurement models:** Opting for a vendor-neutral, requirements-based approach allows agencies to choose from a wider variety of solutions to meet their price, performance, and flexibility needs. In acquiring those solutions, agencies can stretch resources by using an alternative "pay-as-you-go" approach that spends operational expense (OpEx) dollars rather than capital expense (CapEx) funds. This approach can even subsidize existing costly operational support costs like maintenance. Utilization-based models, in contrast to capital procurement, allow agencies to scale in order to meet ever-changing demand and upgrade based on needs instead of appropriation cycles.
- **Invest in technologies and vendors with a clear path forward:** Work with and deploy only the solutions with a defined migration plan to the New IP.

The New IP empowers agencies with user-centric solutions and evolutionary architectures that promote self-service innovation. Studies also project that modernizing network systems and procurement strategies can save federal IT organizations up to $7 billion over the next five years. The New IP promotes collaboration among an ecosystem of vendors to collectively accelerate the pace of federal IT innovation. The New IP can address the risks associated with outdated networks while delivering significant performance, cost, and security improvements.

The New IP requires networks that are open and standards based, encompassing on-demand flexibility that provides both technical and business agility. It is not tied to single vendors or brands, useful life cycles or term commitments. It manifests in a live and fluid environment and the

Figure 4: The New IP is Transforming IT.



New IP network becomes a strategic enabler of scale, scope, and speed to services and applications.

Multivendor Solutions Promote Innovation and Accountability

The government has realized that competition is the driving force behind innovation and value. Single sources of supply do not create the competition necessary to achieve assertive innovation and value. True competition in IT only occurs when competing manufacturer brands are sought and evaluated in solutions. To provide competition in networking, multiple manufacturers must be considered and used for similar network functions. Unfortunately, in government acquisitions, infrastructure purchases are often driven through a small number of resellers offering solutions from the same brand manufacturer or vendor. These resellers are mistakenly viewed as multiple vendors with alternative solutions. By limiting choice, this process is limiting competition, thereby reducing innovation and increasing cost.

Gartner validated that "networks based on a single vendor are vastly more expensive to operate and maintain than modern, multivendor networks" that are often utilized by high performing Fortune 500 companies and enterprises with sustained demands for high-performance, cost-effective service. According to Gartner Research, "the introduction of a second vendor into the network reduces the Total Cost of Ownership (TCO) by 15 to 25 percent over a five-year period.[10]"

This was more recently validated in a study by Meritalk of over 200 government IT professionals and decision makers.[11]

According to the research, that portion of the budget earmarked for network service could ultimately realize substantial savings and improved performance and reliability if a conscientious reduction of unintentional vendor bias was exercised as a standard program objective. By investing in efforts to minimize vendor bias, the government could yield billions in savings by:

- Moving from single-supplier Original Equipment Manufacturer (OEM) to multivendor standards based open heterogeneous networks
- Defining acquisition requirements in terms of features, functions, capabilities, and service levels without specifying brands or referencing particular vendors.
- Investing in network technologies that enhance and improve mission outcomes through agility, open interoperable systems, automation, simplified management, and security

Agencies can take simple steps that make a big difference. Based on the actual experience of federal users, infrastructure independence pays off with 94 percent of agencies with multiple vendors claiming savings tied specifically to that approach.[12]

Competitive, multi-manufacturer procurement drives down pricing in both the short-term and long-term. Forced to bid against competitors, vendors must innovate and lower their prices to win Request for Proposals (RFPs). Gartner found that capital costs fell 30 to 50 percent when a second infrastructure vendor was introduced. RFP requirements that specify a brand or specific "vendor-like" features and capabilities do not do enough to ensure competition as they inherently imply a bias towards the referenced vendor.

Leveraging Contracting to Increase Competition and Reduce Costs

At the same time, multivendor and multi-manufacturer competition ensures that the cost of every service contract, upgrade, and training program in the future is made in the context of competitive pricing.

Competitive pricing is available on government wide acquisition contracts (GWACs) from NITAAC CIO-CS, SEWP V and GSA. Agencies are also using their own Multiple Awards Contracts (MACs). Both of these types of contracts ensure that contract holders are vetted. All agencies need to do to maximize innovation and value is to ensure the acquisition provides the opportunity for competing manufacturer solutions, not just contract holders.

For example, in 2014 the Department of Commerce awarded its first multivendor and multi-manufacturer enterprise wide contract for Networking Equipment and Support Services. It was standards-based and included multiple awards for the purpose of reducing the cost of enterprise network equipment by 20 to 25 percent annually.[13] According to the Department's own announcement, "The new contract, which is for network equipment and maintenance, is expected to save up to $25 million in taxpayer dollars over the next five years. It also streamlines the procurement process, reduces the time needed to award hundreds of separate contracts to do the same tasks, and creates partners in companies that are capable of offering discounts and exceptional service.

[10] Gartner, "Debunking the Myth of the Single-vendor Network," November 2010 https://www.gartner.com/doc/1471937

[11] MeriTalk, "Infrastructure Independence, Set My IT Free," March 2013 http://www.meritalk.com/infrastructureindependence

[12] MeriTalk, "Infrastructure Independence, Set My IT Free," March 2013 http://www.meritalk.com/infrastructureindependence

[13] Department of Commerce announcement http://www.commerce.gov/blog/2014/05/14/commerce-department-supports-small-businesses

Reliance on a single network hardware vendor also hurts network performance. By modernizing network infrastructures, agencies can relinquish vendor or OEM-equivalent dependencies in favor of open, interoperable, standards-based network equipment. As a result, they can increase network agility and take advantage of a wider range of innovative tools for monitoring and managing their networks.

"In addition to saving money, these contracts support small businesses and the Department's efficiency, enabling Commerce to focus more resources on our primary mission to support American businesses, help create jobs and strengthen the economy."

By applying new network architectures, management tools, and open-standard protocols, agencies require less network service. In an era where network traffic continues to accelerate, and where agency network managers often find themselves behind the growth curve, 44 percent of multivendor agencies correlate having more vendors with better network performance.[14]

Surprisingly, while the government strongly advocates for open standards and competition in acquisitions, its network infrastructure does not reflect it. A fundamental problem faced by agencies is that a large portion of federal government networks are designed around proprietary protocols supported by a single vendor. The federal government has spent an estimated $70 billion on network infrastructure and maintenance in the last decade and eighty-six percent of that spending has gone to a single networking supplier.

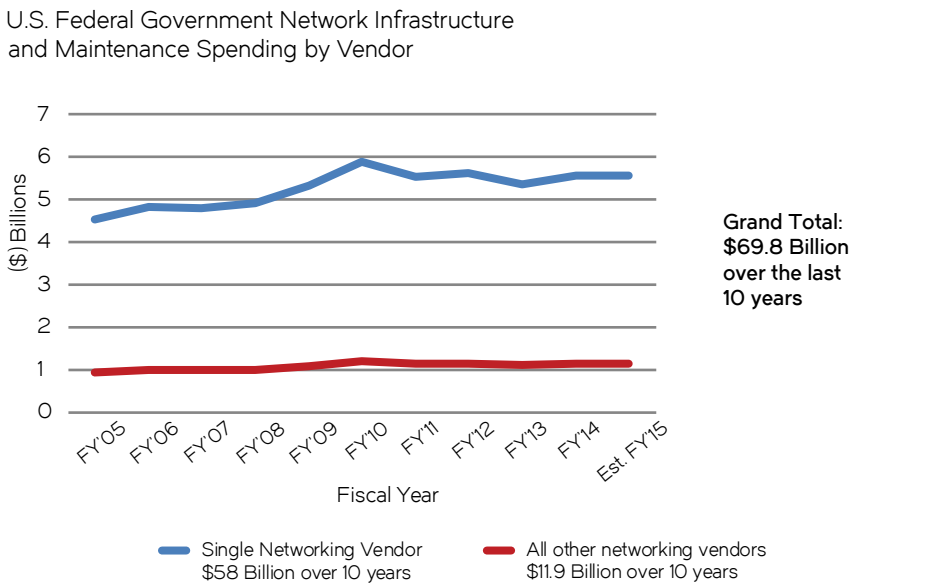


Figure 5: U.S. Federal Government Spending in the Past Seven Years.

The lack of distribution in spending is unexpected given the number of capable vendors in the highly competitive networking space. In comparison, the largest server manufacturer—HP— owns just 26 percent of the server market[15] and the largest Systems Integrator (SI)—Lockheed Martin—owns just 13 percent of SI market share.[16] Even the iPhone with its popularity commands just 40 percent of the US market and even less of the global market that it essentially created.

In keeping with basic economics, less competition drives higher prices. Agencies pay more for initial purchases, more for service contracts, more for training, and more for future product upgrades. Monopolies are invariably bad for consumers–all consumers.

Government clearly recognizes these facts, as the Federal Acquisition Regulations (FAR) support competition and open standards-based approach. It can help break the cycle of status quo IT acquisitions and continual, ever-escalating maintenance and support costs versus new investments. The FAR requires promoting competition to the maximum extent practicable, prohibiting agencies from soliciting quotations based on personal preference, or restricting solicitations to well-known and widely distributed makes or brands in FAR's 13.104 and 6.101. The FAR even takes the requirement a step further by defining the restrictions and onerous actions that an agency must take when using brand names in acquisitions as necessary to meet unique mission needs in FARs 6.302-1, 13.106-1, 13.501, 16.505(a)4.[17]

[14] Op. cit. MeriTalk

[15] IDC Worldwide Quarterly Server Tracker report, http://www.idc.com/getdoc.jsp?containerId=prUS25288114

[16] https://www.fpds.gov/fpdsng_cms/index.php/en/reports/62-top-100-contractors-report3.html

[17] http://www.acquisition.gov/far/

State and local governments seem to be struggling with similar challenges. According to the San Jose Mercury News San Jose State University did not bid out its $28 million network project, which cost more than the entire California State University system's $22 million networking upgrade.

Source: http://www.networkworld.com/article/2858636/cisco-subnet/cisco-sjsu-we-cant-hear-you.html

Recently passed, as part of the National Defense Authorization Act for Fiscal Year 2015, was the Federal IT Acquisition Reform Act (FITARA), which will also help to have a positive impact on IT effectiveness and acquisitions. It is a measure to reduce waste in government IT spending by increasing the authority of federal CIOs.[18]

For FY 2015, the budget includes $20 million for Information Technology Oversight and Reform (ITOR). This fund, previously known as the Integrated, Efficient, and Effective Uses of Information Technology (IEEUIT), will use data, analytics and digital services to improve the efficiency, effectiveness, and security of government operations and programs.[19] The ITOR fund's objectives are to:

1. Improve the effectiveness of government programs by developing federal digital services that provide a world-class customer experience to citizens and businesses
2. Reduce waste, duplication, and inefficient uses of IT through data-driven investment management
3. Improve oversight of federal cybersecurity and advance the cybersecurity posture of federal systems and data

Emerging Technologies Require Open Standards

Today's networks will be open, more agile, and secure. They will be built from a multivendor ecosystem with open standards based-architectures. Agencies are quickly moving to the mindset that views IT as a strategic asset that drives cost savings by providing new and emerging technologies that can improve the way the government does business and delivers services.

New, emerging technologies are promoted by mandating and enforcing the use of open industry standards. These standards need to be consistent with the directive in the Revised OMB CircularA-119 establishing policies on federal use and development of voluntary consensus standards, as well as conformity assessment activities in support of the Memorandum for The Heads of Executive Departments and Agencies, M-12-08. This memorandum deals with the use of consensus standards, specifications, and formats in compliance with Federal Government Objectives for Standards Engagement to Address National Priorities.[20]

Over-prescriptive requirements often referencing specific brands continue to perpetuate the problem by extending the costly cycle of proprietary vendor lock-in as reported in "Billions in the Balance" by the Public Spend Forum.org, and highlighted in the recent paper by MITRE Corporation, "Gaining Leverage over Vendor Lock to Improve Acquisition Performance and Cost Efficiencies."

Status quo IT acquisitions will not allow agency CIOs to transform and modernize networks in support of their current IT mission priorities to deliver on six key objectives:[21]

- Consolidate data centers
- Reduce inefficiencies through shared services and strategic sourcing
- Improve mobility
- Leverage IT as a Service (ITaaS) and cloud

[18] FITARA Included in NDAA Bill http://oversight.house.gov/release/fitara-included-ndaa-bill/

[19] http://www.whitehouse.gov/sites/default/files/omb/assets/organization/fy2015_omb_budget.pdf

[20] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf and http://www.whitehouse.gov/omb/circulars_a119

[21] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2014_budget_priorities_20130410.pdf

- Exploit Big Data and analytics
- Ensure cyber security

While it is often believed, and justified in practice through government acquisition, that consolidating networks with a single vendor boosts interoperability and reduces operational expenses, real data and past history reveals the opposite.

Reduce Training, Maintenance, and Personnel Costs

Gartner found that organizations were actually able to dramatically simplify their networks by adding new vendors. Where single vendor networks had substantial legacy hardware, multivendor networks tended to be made of interoperable components based on open standards, and agencies observed savings ranging from 40 to 95 percent.[22]

Furthermore, architectures based on open standards drive down lifecycle costs, speed up time to deliver new capabilities, and are less disruptive to upgrade because aging elements are easier to replace. Closed, proprietary, and monolithic systems usually require complete reengineering to take advantage of new capabilities, or the costly requirement for a supply of legacy components to keep the existing system operational.

Flattening and automating network architecture—a hallmark of modern networks—dramatically reduces training, maintenance, and personnel costs. Standardizing on a single brand network is not making the job easier for the consumer. It is however, making it easier for the manufacturer while the consumer still carries all their burdens.

In addition, modularity helps by "managing complexity by breaking complex systems into discrete components which can then communicate with one another only through standardized interfaces is made possible in systems using open standards. When combined with a 'service-oriented' approach, this can give a low risk way of retaining useful legacy systems that work with new components. Increasing the modularity of systems brings important benefits.

The possibility of smaller companies becoming involved in modular IT projects increases the choice of contractors available to the customer. Components based on open standards help implementers and end users integrate new components, capabilities, and applications with existing systems."[23] Environments using open standards help create a larger talent pool to leverage, also driving down the costs of training and support.

Software-Defined Networking Uses Open Protocols

SDN is an approach to using open protocols, such as OpenFlow, to apply globally aware software control from edge to core network devices that traditionally use closed and proprietary firmware.

SDN offers the ability to separate the control from the data forwarding functions to drive automation and policy enforcement. SDN controllers automate and centralize configurations of network elements such as switches, routers, and firewalls to reduce manual processes and errors. Additionally, SDN controllers can centralize and enforce policies across existing network hardware devices and

Recognizing this dilemma the former Assistant Secretary for Information and Technology and CIO for the Department of Veterans Affairs, demonstrated exceptional leadership with an agency-wide mandate in a memo titled, "VA: Open Standard Protocols for VA Networks." In this memo, key statements included the following:

- Codifying the decision to migrate from proprietary protocols to open standard protocols on VA's data networks, in order to enable participation from any vendor
- Migrating to open standard protocols supports cost containment strategies, and will increase VA's flexibility and ability to interoperate with multiple vendors
- Enable rapid advances in network infrastructure capabilities at the lowest possible costs with improved interoperability, innovation, and open competition

Source: Veterans Affairs CIO Memorandum August 2012 iehrsummit.dsigroup.org/breaking-news/?goback=%2Egde_4115936_member_149976515

[22] Op. cit. Gartner "Debunking the Myths of Single Vendor Networks"

[23] Open Standards in Government IT: A Review of the Evidence: An independent report for the Cabinet Office by the Centre for Intellectual Property & Policy Management at Bournemouth University

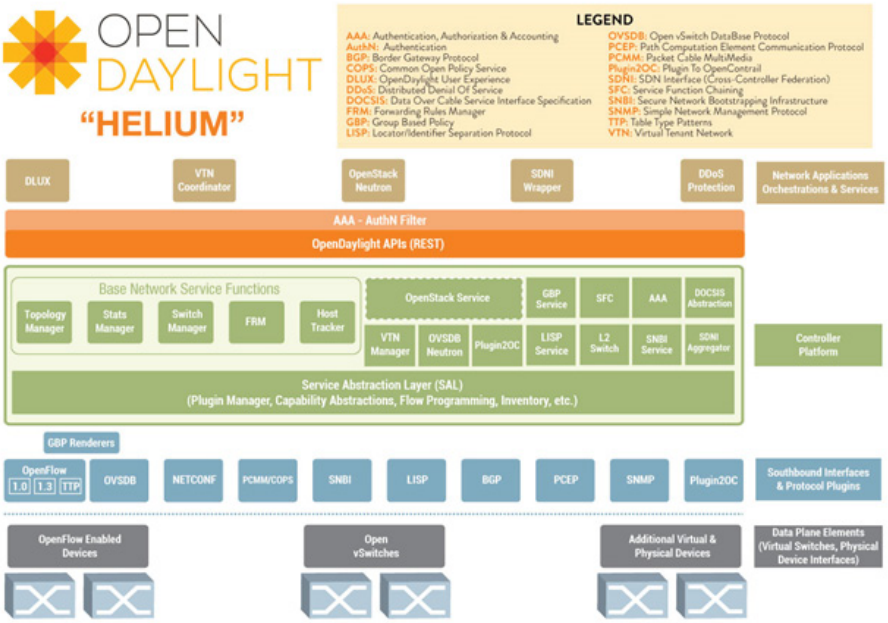


Figure 6: OpenDaylight Helium Network.

NFV instances. Increased visibility of the network and automation offer the ability to reduce operational time and money within the network.

SDN controllers are based on open standards and offer high levels of programmability to develop network and security centric applications to increase capabilities of a modern SDN-enabled network. SDN offers numerous benefits including on-demand provisioning, automated load balancing, streamlined physical infrastructure, and the ability to scale network resources in lockstep with application and data needs.

As federal IT leaders have learned over the last decade, successful virtualization depends heavily on compatible infrastructure elements—including network, storage, and servers. That compatibility relies on open standards and open platforms. Much like legacy applications impede efforts to virtualize servers, proprietary and legacy networks will prevent successful network virtualization. As such, building networks on open industry standards today will provide vast cost savings opportunities in the future—and at no incremental cost.

SDN benefits include: Service provisioning speed and agility, network flexibility and holistic management, improved and more granular security, efficient and lowered operating expenses, and virtual network services with lowered CapEx.[24] Using server virtualization as a model, adjusted for relative share of IT spending, network virtualization may deliver potential savings of 8.9 percent of total IT budgets.[25]

Fabrics are Evolutionary

Ethernet fabrics are foundational and can help accelerate the transformation of networks. A fabric is a unified switching architecture that provides transport through individual devices acting together as a single logical entity. The hallmarks of a fabric are simplified operations, highly automated provisioning, and perfect resource utilization. They can help agencies deploy network capacity five times faster and increase network utilization by 200 percent. An Ethernet fabric is an essential underlay network architecture that enables the New IP and an agile business. A fabric-based underlay increases agility by reducing complexity and increasing automation saving up to 50 percent on OpEx. Fabrics are agile and automated, and they easily scale up and out, adapting to handle instantaneous changes in traffic flows, flow sizes, packet sizes, and protocols. Fabric architectures provide important network capabilities that:

- Utilize a true democracy to significantly reduce the time to deploy new services and provide unsurpassed availability. They are flat architectures, without hierarchy in which every switch is equal to every other switch so that there is no single point of failure. They provide self-forming and self-healing networks where all paths are equal and available.
- Provide distributed intelligence to remove the need for time-consuming, labor-intensive, and error-prone manual network reconfiguration. Every port is aware of every other port allowing you to move workloads with their associated characteristics with the Automatic Migration of Port Profiles (AMPP). These characteristics can automatically

[24] InformationWeek article by Serdar Yegulap 7/12/2013 "Five SDN Benefits Enterprises Should Consider" http://www.networkcomputing.com/networking/five-sdn-benefits-enterprises-should-consider/a/d-id/1234292?

[25] IDC, "The Economics of Virtualization: Moving Toward an Application-Based Cost Model"

and seamlessly be moved to ensure continued consistent delivery of services including access control, Quality of Service (QoS), and other port-oriented application characteristics.

- Deliver native automation from the ground up, making them five to ten times faster to deploy than individual elements and providing a wide range of additional capabilities such as AMPP, zero-touch provisioning for virtual machines (VMs), network self-configuration, and near-perfect load balancing.
- Enable absolute persistence optimizing and maximizing the flow of traffic in real time, reacting to changing demands, transparent balancing workloads, and ensuring availability.
- Perform without compromise between scale and latency. Fabrics provide speed by taking the most efficient path, automatically and continuously.
- Simplify integration with surrounding technologies like overlays, making them simpler and more efficient. Fabrics make underlay-overlay integration more robust by combining a single integration point with inherent distributed intelligence.

Embrace Innovative Technology

New technologies such as Ethernet fabrics, SDN, NFV and open-source software-based solutions (like OpenStack and OpenDaylight) leverage open standards, spawn innovation, reduce complexity, and help eliminate vendor lock-in, further reducing total costs.

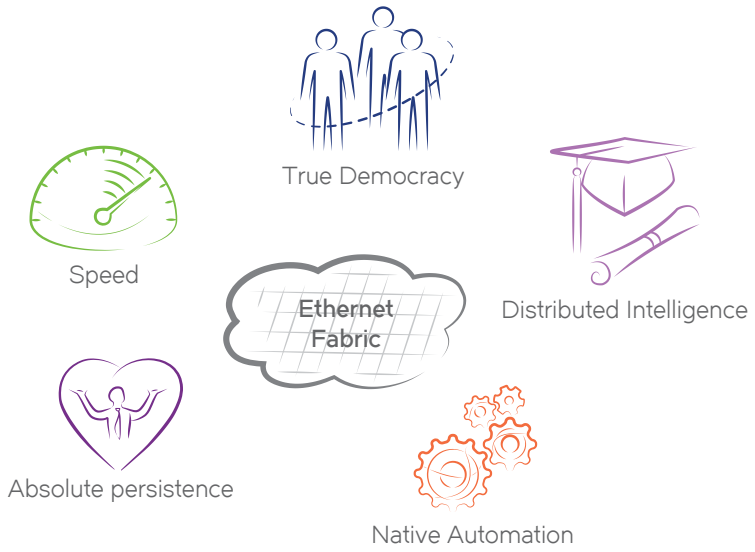
Significant innovation is not only achieved through open standards and competition. It is realized by tapping into the collective expertise of all IT users and developers worldwide. Standards are required to keep the choices open so that innovation can be capitalized on from wherever it originates. The open source community is global and united in its effort to promote and protect open-source software, development, and communities. By design, open source creates options and maintains flexibility. Sourcing all of the advances in innovation, software, and technology is the only way to ensure to keep pace with today's rapidly changing IT environment.

According to Deloitte Consulting, SDN alone may reduce networking costs by as much as 50 percent and cut 7.5 percent from total IT budgets.[26] It does so by simplifying management of the network through centralized policies and creating an environment that can quickly adapt and deploy new applications, technologies, and innovations.

Virtualization of compute and storage has saved organizations significant dollars by moving from special purpose systems to virtualized "Common Off-The-Shelf" (COTS) servers. A similar movement is now taking place in networking and it will manifest itself in the New IP.

Other innovations, like NFV are moving network services (Layer 2 through Layer 7) from special purpose devices to COTS servers, offering the similar efficiency and financial benefits to SDN. An independent publication, SDN Central, conducted a NFV price performance test in October 2014 and determined that a virtualized Layer 3 Router is able to achieve 80 Gbps throughput on a single virtualized machine. The system under test offered a 73 percent cost reduction compared to a standard industry special purpose hardware device.[27] NFV performance improvements continue throughout the stack offering comparable performance

Figure 7: The Benefits of Ethernet Fabrics.



[26] The Economist, Network Effect http://www.economist.com/news/business/21568435-software-defined-networking-inspiring-hope-and-hype-network-effect

[27] SDNCentral NFV Performance Test Validates 80-Gbps https://www.sdxcentral.com/articles/featured/nfv-performance-test-validates-80-gbps-brocade-vyatta/2014/10/

"According to the Mandiant M-Trends Report 2014, the average number of days that attacks were present on a victim's network before being discovered was 229—more than seven months."

Source: http://www.itgovernance.co.uk/media/press-releases/cyber-security-breaches-can-go-undetected.aspx?utm_source=social&utm_medium=twitter#.VUvcnPnF_zg

to special purpose network applicants coupled with open standards and highly agile deployment models.

SDN and Fabrics Provide Increased Network Security and Data Privacy

The risks that cyber-attacks and hacking pose to national security have never been greater. This is a consequence of ever-growing dependency on networks and information technology across all government agencies and businesses. The need to ensure data security and privacy in the network is equally a concern of individuals. Protecting networks and IT infrastructure is critical.

Major technology and cultural shifts that are taking place around mobile devices, the cloud, and social media are having a tremendous effect on the network. Changing end-user expectations drive new application architectures, service deployment models, and infrastructure needs such as virtualization. However, as organizations seek to meet these demands, they also face the challenge of delivering increased productivity at a reduced cost while maintaining service and increasing security levels.

A comprehensive security undertaking needs to cover users, data, applications, and the entire networking infrastructure. Ensuring data privacy, controlling the digital footprint and threat detection and prevention are leading security concerns for all organizations. The networking infrastructure, which includes both physical and virtual elements for switching, routing, and appliances for application and security services, must play an integral part in security and privacy policy.

A robust hardware network infrastructure is a critical element of a comprehensive security strategy. Fabric switches offer an advanced way to automate, simplify, and centralize policy management and control, offering a more seamless platform for the insertion of security devices and services while increasing performance and reliability. Fabrics remove overly complicated, inefficient, and highly manual requirements of traditional networks, which significantly reduces the potential for conflicts, security vulnerabilities, and outages due to human error.

Many network switches also now include built-in or optional data encryption, utilizing both MacSec and IPSec. Commercial network encryption and data privacy solutions, in particular those utilizing the Suite B algorithms, and those products participating in the Commercial Solutions for Classified (CSfC) Programs, are making highly secure network encryption far more cost-effective and viable. The best of this new class of IPSec products are capable of operating at wire speed up to 10 Gbps and higher (through link aggregation techniques).

In addition, virtualized (NFV) VPNs offering can secure data all the way to the virtualized application in the data center, protecting an area of the network that is typically operating in the clear and thus more vulnerable. Other virtualized security functions, such as stateful firewalls, IDS/IPSs, authentication, Web filtering, and proxy AV, can now be embedded deep into the network, into areas where security typically has not reside (such as on the data center server edge), directly protecting applications and Virtual Machines (VMs). Furthermore, each instance of a virtualized security

function can have granular policies and configurations for a specific customer (called multitenancy) or application. Extending security to the data center edge adds a new layer that does not exist today, deepening the defense-in-depth posture.

Modernized network hardware is taking on some additional and important roles in the overall security architecture, and a new network services overlay (including SDN and NFV) is providing continuous monitoring, advanced visibility, reach, and the capability to protect privacy and assets in cyber space. Automated systems, as well as any cyber security personnel, can use the improved visibility to make more accurate decisions preventing and addressing cyber threats more quickly.

Leverage Procurement Processes to Provide Limitless Upgradability and Scalability

Shifting from IT as an asset to IT as a Service (ITaaS) allows agencies to streamline delivery as well as minimize OpEx expenditures. A recent example of this shift in acquisitions can be found in the Defense Information Systems Agency (DISA)'s award of Enterprise Storage Services (ESS II) valued at $427 million to provide "information storage infrastructure of 'on demand' enterprise services for specified operating environments," according to the Department of Defense contract announcement.[28]

Another example can be found in the Central Intelligence Agency (CIA)'s move to the cloud with a large private cloud contract procurement valued at $600 million. According to the CIA's Chief Information Officer, "We're…putting together this public cloud on private premises. The idea is to be able to take the best of the public sector—we're going to lift it and sort of place it behind our fence line, if you will, but then be able to operate them for the intelligence community on our premises."[29]

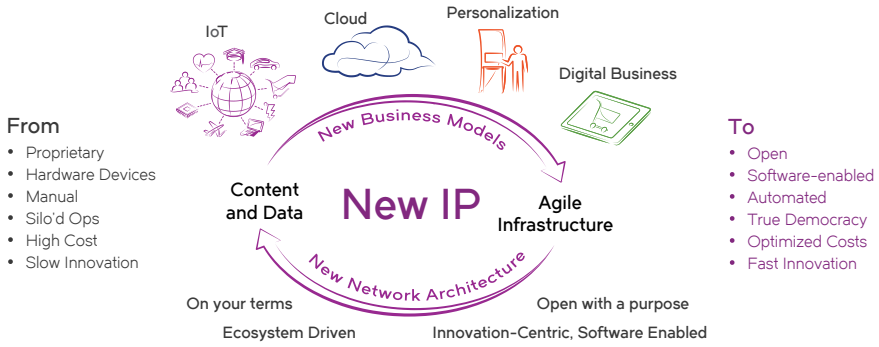


Figure 8: The New IP Accelerates Service Delivery, Data Access, and Innovation.

Utilization-based models, in contrast to capital procurement, allow agencies to scale in order to meet ever-changing demand and upgrade based on needs instead of appropriation cycles. Subscription services allow users to acquire: what they need, when they need it and where they need it. Benefits include improved mission outcomes through agility, and the ability to deploy new applications rapidly to meet changing priorities. Agencies can eliminate inefficiencies by paying only for assets that meet current needs and are being fully utilized. They can transform expensive legacy support costs into new agile networks.

The Next Move

The risk of not modernizing, evolving, and transforming the network is far greater than any risk and cost associated with changing the status quo single vendor IT and network culture. The task is not easy. Agency leaders will need to:

1. Demonstrate leadership to drive change and disrupt the status quo culture to achieve network modernization objectives.
2. Mandate and enforce the use of open standards in network implementations and prohibit the use of proprietary protocols in networks.
3. Increase market research and link requirements to agency mission outcomes defined as functions, capabilities and service levels that completely avoid the use of brand name references.
4. Embrace multivendor/multi-manufacturer standards based network implementations to ensure flexibility, innovation, and competition to return the best value and lower the cost of networking.

[28] Department of Defense Contract Announcements December, 19 2014 http://www.defense.gov/contracts/contract.aspx?contractid=5442

[29] CIO.Com Article, CIA Off and Running With Amazon Web Services http://www.cio.com/article/2375269/hybrid-cloud/cia-off-and-running-with-amazon-web-services.html

5. Be agile; refocus OpEx funds from aging infrastructure support to leverage new acquisition models like ITaaS and cloud enablement. With limitless upgradability, scalability, and agility, agencies can eliminate waste and ensure that they deploy exactly the assets and technology they need, when and where they need it.
6. Adopt a strategic approach, rather than a product- or vendor-oriented approach to IT and networking investments. This means leveraging new companies and technologies to build secure large and scalable environments at lower cost, with interoperable multi-manufacturer network elements based on open standards and application programming interfaces.
7. Train and educate the workforce to embrace and encourage competition by harnessing the Federal Acquisition Regulations (FAR).

The result will be a significantly more agile, innovative, and secure network infrastructure that is less complex and easier to manage for agencies; one that enhances mission outcomes, promotes innovation and thrives on competitive marketplace to reduce overall costs.

For more information about Brocade solutions, visit www.brocade.com/federal.

For more information about the government Open Source Center, visit opensource.gov.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE